

Ochrana vašich dat

Jak EY zajišťuje
ochranu osobních údajů
a bezpečnost informací



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



Shape the future
with confidence

V EY jsme přesvědčeni, že dobrá pověst podniku je podmíněna spolehlivými mechanismy ochrany dat a zabezpečení informací. Ochranu dat a zabezpečení informací považujeme za základní součásti podnikání. Naším cílem je chránit informace, osobní údaje a klientská data. Jsme přesvědčeni, že spolehlivé mechanismy ochrany dat a zabezpečení informací jsou pro poskytovatele odborných poradenských služeb zcela zásadní. Účelem tohoto dokumentu je přiblížit zásady, které v dané oblasti uplatňujeme, konkrétně jak k zabezpečení informací týkajících se klientů přistupujeme a jaké informační systémy za tímto účelem využíváme. Specifika souvisejících opatření se mohou lišit v závislosti na poskytovaných službách a příslušných regulačních požadavcích dané země. Naše programy a postupy ochrany dat a zabezpečení informací jsou koncipovány tak, aby sdílení údajů probíhalo odpovídajícím způsobem a v souladu s platnými právními předpisy a zároveň byla zachována důvěrnost, integrita a dostupnost těchto informací.



Promyšlená strategie zabezpečení informací a ochrany osobních údajů

EY poskytuje fungující, stabilní a vysoce kvalitní služby klientům po celém světě. Bez účinné strategie v oblasti ochrany dat a zabezpečení informací by toto nebylo možné. O ochranu informací, osobních údajů či dat klientů usilujeme za všech okolností – ať již jde o jejich vytváření, zpracování, přenos nebo uchovávání. V rámci efektivní správy těchto položek průběžně kontrolujeme dodržování platných národních i mezinárodních regulatorních norem. Za řádné provádění programů a postupů týkajících se ochrany osobních údajů a zabezpečení informací odpovídají dva samostatné úseky EY, jež však mezi sebou úzce spolupracují: Globální síť pro ochranu osobních údajů a Globální organizace pro bezpečnost informací. Jejich úkolem je chránit informace EY a klientů EY před neoprávněným shromažďováním, uchováváním, používáním, zveřejňováním, úpravami či zničením. Za tímto účelem prosazují odpovídající zásady, standardy, postupy, pokyny, technologické a administrativní kontroly, včetně průběžných školení a zvyšování povědomí zaměstnanců společnosti. Globální týmy EY pro ochranu osobních údajů a pro bezpečnost informací postupují ve vzájemném souladu, pokud jde o globální priority uplatňované v rámci celosvětové sítě EY. Ve spojitosti s ochranou informací, osobních údajů a klientských dat se tak orientujeme dle jednotné a soudržné vize.

Uplatňovaný rámec ochrany osobních údajů

Rámec ochrany osobních údajů, jímž se společnost EY řídí, vychází z platného práva (včetně obecného nařízení EU o ochraně osobních údajů (GDPR)), dalších regulačních požadavků a příslušných profesních standardů. Je založen na závazku všech členských firem EY chránit osobní údaje a důvěrné informace (včetně klientských informací) dle následujících zásad:

- **Zákonnost, spravedlnost a transparentnost:** s veškerými osobními údaji nakládáme způsobem, který je etický, přiměřený, jasně sdělený a zákonný.
- **Omezení účelu:** osobní údaje používáme pouze pro definované a schválené účely.
- **Minimalizace údajů:** shromažďujeme a zpracováváme pouze ty osobní údaje, které jsou nezbytné pro daný účel.
- **Přesnost:** ověřujeme, že jsou osobní údaje přesné a v potřebné kvalitě dle navrhovaného účelu.
- **Omezení uchovávání:** osobní údaje uchováváme pouze po dobu nezbytnou k dosažení účelu, pro který byly shromážděny.
- **Integrita a důvěrnost:** ověřování, že osobní údaje jsou uchovávány bezpečně a důvěrně a že přístup k nim je kontrolován na základě přísného principu „potřeby vědět“.
- **Odpovědnost:** prokázání souladu se zásadami ochrany osobních údajů v souladu s Globální směrnicí EY o ochraně osobních údajů a důvěrnosti informací a Globálním etickým kodexem EY.
- **Citlivé informace:** zvýšená opatrnost při zpracování zvláštních kategorií osobních údajů nebo citlivých informací o klientech.
- **Externí zpracovatelé:** ověřování, zda třetí strany, které naším jménem zpracovávají osobní údaje nebo důvěrné informace, včetně údajů o klientech, jménem organizace EY, přijaly rámec ochrany údajů, který zajišťuje odpovídající ochranu těchto údajů, a zda smlouvy s těmito třetími stranami obsahují podmínky ochrany údajů v souladu s platnými právními předpisy.



Prvky našeho rámce pro ochranu osobních údajů

Mezinárodní předávání osobních údajů

Mezinárodní předávání osobních údajů je přísně regulováno klíčovými zákony a předpisy na ochranu osobních údajů (**například evropskou legislativou o ochraně osobních údajů**). Různé právní předpisy o ochraně osobních údajů po celém světě zakazují předávání osobních údajů do zahraničí, pokud předávající organizace nezavede příslušná bezpečnostní opatření. Tým EY využívají schválené mechanismy předávání osobních údajů, aby vyhovely právním předpisům na ochranu osobních údajů. Při předávání evropských osobních údajů do zemí mimo Evropský hospodářský prostor, které nemají komplexní legislativní přístup k ochraně údajů, takže podle EU neposkytují dostatečnou úroveň ochrany práv jednotlivců na soukromí, také bereme v úvahu rozhodnutí Soudního dvora Evropské unie (SDEU) ve věci Schrems II.

- Tým EY provádějí posouzení dopadu přenosu dat na místní zákony a postupy a v případě potřeby zahrnují vhodná doplňková opatření k ověření adekvátní ochrany osobních údajů.
- Tým EY zavedly závazná podniková pravidla (BCR) pro činnosti správce i pro činnosti zpracovatele jakožto mechanismus umožňující mezinárodní předávání osobních údajů mezi členskými firmami EY. BCR nám pomáhají plynule předávat osobní údaje v rámci členských firem EY, což usnadňuje spolupráci mezi jednotlivými týmy. BCR, které se vztahují na všechny členské firmy EY po celém světě, jsou zveřejněna na adrese https://www.ey.com/en_gl/legal-and-privacy/data-protection-binding-corporate-rules-program.
- Členské firmy EY dále využívají schválené standardní smluvní doložky (SCC) ve smlouvách s klienty a třetími stranami, je-li to vhodné.
- Ernst & Young LLP, USA, a její přidružené subjekty v USA dodržují Rámec ochrany soukromí mezi EU a USA, rozšíření Rámce pro ochranu soukromí mezi EU a USA pro Spojené království a Rámec pro ochranu osobních údajů mezi Švýcarskem a USA, které zveřejnilo Ministerstvo obchodu USA. Další informace naleznete zde [Ernst & Young LLP EU-US Data Privacy Framework Privacy Statement](#).

Odpovědná AI

Nové technologie, zejména umělá inteligence (AI), zažívají bezprecedentní růst s obrovským transformačním potenciálem. Tento rychlý rozvoj však může přinést nové nebo zesílené výzvy včetně nových právních a regulačních požadavků, nových nebo zvýšených rizik v oblasti ochrany osobních údajů, etických otázek a potřeby robustních rámců pro správu AI. Ochrana osobních údajů je nedílnou součástí našeho rámce odpovědné AI a přesahuje pouhé dodržování předpisů až po začlenění zásad ochrany dat do základů návrhu, vývoje a používání AI. EY se zavazuje k odpovědnému používání osobních údajů a důvěrných informací (včetně informací o klientech) v technologiích AI v souladu s platnými zákony, předpisy a profesními standardy, které se vztahují na používání a správu systémů AI a souvisejících dat. Další informace naleznete v [zásadách odpovědné AI společnosti EY](#).



Sladění priorit v oblasti ochrany údajů a bezpečnosti informací odpovídá jednotné a soudržné vizi, kterou ve spojitosti s ochranou informací, osobních údajů a klientských dat EY globálně prosazuje

Školící a osvětové programy

Spolu s tím, jak se mění metody útoků, je zapotřebí přizpůsobovat také obsah informací, pokynů a školení, které našim lidem poskytujeme. Zvyšování povědomí o hrozbách týkajících se ochrany soukromí a informační bezpečnosti a podpora našich odborníků v odpovědném využívání nových technologií, včetně umělé inteligence v souladu s měnícími se zákony, předpisy a profesními standardy představuje průběžný a dynamický proces. Důležitost, již mu přikládáme, se odráží nejen v povinných školeních, která pravidelně aktualizujeme pro každou servisní divizi EY, ale i v mnoha dalších činnostech, jejichž cílem je zvýšit povědomí o dané problematice v rámci globální komunity EY.

Globální zásady společnosti EY v oblasti zabezpečení informací

Naše zásady v oblasti zabezpečení informací, včetně podpůrných standardů a kontrol, jsou průběžně prověřovány vrcholovým vedením. Tak je zajištěno, že jsou stále aktuální a přesné a že odpovídají právním a regulačním požadavkům, které se na společnost EY vztahují. V souladu s uznávanými rámci, jako je ISO 27001, se předepsané či doporučené zásady týkají řady široce uznávaných oblastí informační bezpečnosti, mimo jiné z následujících oblastí:

- Kontrola a přístup
- Správa aktiv: klasifikace a kontrola
- Bezpečnost komunikace, sítí a provozu
- Bezpečnost lidských zdrojů: personál
- Zajištění, vývoj a údržba systémů informační bezpečnosti
- Fyzická a environmentální bezpečnost
- Řízení rizik

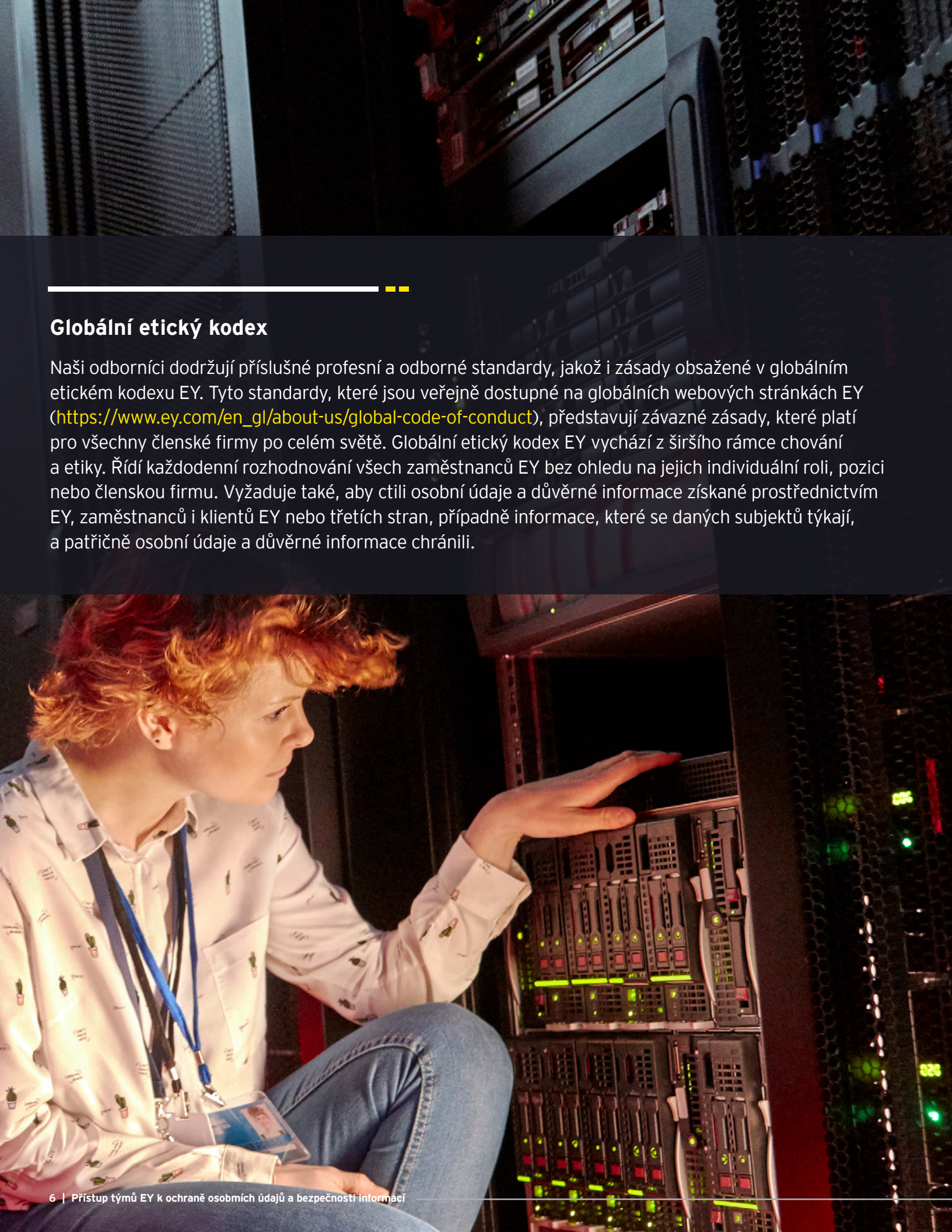
Důraz na technické aspekty zabezpečení

Náš přístup k zabezpečení informací není postaven pouze na deklarovaných bezpečnostních zásadách a standardech. Důvěrnost, integritu a dostupnost dat zajišťujeme rovněž prostřednictvím ochrany našich technologických zdrojů a prostředků. Související opatření zahrnují mimo jiné:

- Šifrování disků stolních počítačů a notebooků
- Firewally stolních počítačů a notebooků
- Nástroje na šifrování vyměnitelných médií: přístup k zápisu je buď ve výchozím nastavení blokován, nebo je povolen s šifrováním
- Používání antivirů a softwaru na ochranu proti malwaru
- Vícefaktorové ověřování
- Automatizovaná instalace oprav a hodnocení zranitelnosti zabezpečení
- Důkladné kontroly fyzického stavu, prostředí, sítí a bezpečnostního perimetru
- Technologie detekce a prevence narušení
- Systémy monitorování a detekce

Kromě toho investujeme značné množství času i prostředků do nejmodernějších bezpečnostních technologií. Strategii zabezpečení informací utváříme v souladu s plánem nasazování technologií a nabídkou technologických služeb pro klienty. Bezpečnostním problémům, které by jinak důvěrnost, integritu či dostupnost našich technologických zdrojů mohly ohrozit, dokážeme díky tomu náležitě čelit.





Globální etický kodex

Naši odborníci dodržují příslušné profesní a odborné standardy, jakož i zásady obsažené v globálním etickém kodexu EY. Tyto standardy, které jsou veřejně dostupné na globálních webových stránkách EY (https://www.ey.com/en_gl/about-us/global-code-of-conduct), představují závazné zásady, které platí pro všechny členské firmy po celém světě. Globální etický kodex EY vychází z širšího rámce chování a etiky. Řídí každodenní rozhodování všech zaměstnanců EY bez ohledu na jejich individuální roli, pozici nebo členskou firmu. Vyžaduje také, aby ctili osobní údaje a důvěrné informace získané prostřednictvím EY, zaměstnanců i klientů EY nebo třetích stran, případně informace, které se daných subjektů týkají, a patřičně osobní údaje a důvěrné informace chránili.



Zabezpečení informací

Kontinuita podnikání a obnovy po havárii

Naše trvalé úsilí o ochranu firemních a klientských dat je reflektováno mimo jiné v možnostech obnovy po havárii a zajištění kontinuity provozu v souladu s ISO 22301. Jsme odhodláni chránit zaměstnance, zařízení, infrastrukturu, podnikové procesy, aplikace a data společnosti EY před závažnou událostí, během ní i po jejím výskytu. Postupy, podle nichž postupujeme v reakci na havárii či při obnově systému u kritických služeb, podléhají pečlivé přípravě a testování. Mezi konkrétními metodikami obnovy po havárii a zajištění kontinuity provozních procesů figurují mimo jiné:

- Posouzení dopadu na podnikání
- Plány obnovy po havárii pro kritické úlohy sestavené dle předních odvětvových standardů
- Asistence certifikovaných odborníků pro danou oblast
- Pravidelné testování plánů obnovy po havárii a kontinuity podnikání za účelem ověření provozní připravenosti

Analýza rizik dodavatelského řetězce

V souladu s našimi procesy náležitě péče v oblasti řízení dodavatelů a analyzujeme činnosti třetích stran související s bezpečností informací, nákupem, smlouvami, ochranou údajů a nezávislostí, včetně:

- Hodnocení potenciálních dodavatelů z hlediska souladu s našimi globálními zásadami a kontrolními mechanismy v souladu s normou ISO 27001/2
- Due diligence včetně podrobného zhodnocení rizik a zjištění
- Opatření na snížení dopadů identifikovaných rizik
- Podpora při výběru dodavatelů a sjednávání smluv

K hodnocení inherentních a zbytkových rizik v oblasti zabezpečení informací, dodržování předpisů a dalších kategorií rizik, jako je klasifikace dat, umístění hostingu, přístup a typ přenosu dat, používáme standardní bezpečnostní hodnocení.

Bezpečnostní strategie a odpovědnost

Bez dodržování všeobecných požadavků na zabezpečení informací a etické chování jednotlivců by prosazování komplexně formulovaného programu zabezpečení nebylo možné. Náš program je koncipován tak, aby podněcoval k zachování důvěrnosti, integrity a dostupnosti osobních údajů i klientských dat. Tuto snahu podporujeme prostřednictvím technologií na ochranu dat užívaných v souladu s platnými právními předpisy o ochraně osobních údajů a regulačními požadavky jakož i mezinárodně uznávanou normou ISO 27001/2 pro řízení bezpečnostních programů.

Naše organizace aktivně zajišťuje a řádně spravuje důvěrné a osobní údaje prostřednictvím programu zabezpečení informací založeného na normě ISO 27001/2, který zahrnuje:

- Odpovídající zásady, standardy, pokyny a postupy
- Řízení programu
- Důsledné kontroly zabezpečení technických aspektů
- Zajištění souladu s bezpečnostními požadavky zahrnujícími bezpečnostní kontroly, certifikace a audity
- Jasně vymezená bezpečnostní strategie a definovaný plán zohledňující následující faktory:
 - Ochrana osobních údajů - právní, regulatorní a procesní požadavky
 - Podnikání - předepsané postupy a požadavky
 - Technologie - zásady, normy a postupy
 - Vnější hrozby - sledování vývoje bezpečnostních hrozeb
- Program řízení bezpečnostních incidentů pro účinné řízení a nápravu bezpečnostních incidentů, včetně programu reakce na kritické zranitelnosti v oblasti kybernetické obrany



Dodržování předpisů a auditů

Jako organizace disponujeme globálními programy na ochranu osobních údajů a zabezpečení informací. Využíváme účinný řídicí rámec a dohlížíme na soulad s předpisy prostřednictvím formálních auditů. Při zajišťování našich povinností ohledně ochrany osobních údajů a bezpečnosti informací spoléháme na níže uvedený soubor kontrol a postupů.

Certifikace zabezpečení systémů

Veškeré aplikace a systémy jsou před implementací podrobeny bezpečnostní certifikaci, abychom prokázali, že byly vyvinuty v souladu s našimi globálními zásadami v oblasti zabezpečení informací, jakož i standardy bezpečného vývoje aplikací.

Tento certifikační proces zahrnuje hodnocení rizik, přezkum dokumentace a posouzení zranitelností. Vztahuje se na libovolné aplikace nebo systémy užívané k vytváření, ukládání či správě informací naším jménem a přispívá k zachování důvěrnosti, integrity a dostupnosti údajů společnosti EY a jejích klientů.

Posouzení dopadu na ochranu soukromí a důvěrnost

U aplikací a projektů, které pracují s osobními údaji či údaji o klientech, posuzujeme závažnost dopadů na ochranu soukromí a důvěrnost informací (PIA). V rámci každého takového posouzení je zhodnocena způsobilost dané aplikace či iniciativy vůči globálním standardům a v případě potřeby jsou předložena relevantní doporučení.

Přehled konkrétních opatření na zmírnění rizik, spolu s podrobnými pokyny, je následně po PIA vyhotoven pro všechny uživatele a správce uvedeného systému. Prováděná analýza zahrnuje také přezkum jakýchkoli přeshraničních toků údajů s ohledem na právní a regulační požadavky EU.

Rozsáhlý soubor podnikových zásad a pokynů nám umožňuje vyvíjet aplikace v souladu s platnými standardy a v souladu s požadavky na ochranu osobních údajů.

Posuzování účinnosti kontrol

Abychom ověřili fungování a účinnost zaváděných kontrol, provádíme jejich vícenásobné testy a posudky, mimo jiné jde o následující:

- Analýza zranitelnosti sítí a aplikací, která se zaměřuje na technické aspekty globálních zásad v oblasti zabezpečení informací, jako je správa oprav, bezpečnost aplikací a bezpečnost infrastruktury.
- Hodnocení provozní účinnosti, které přezkoumává technické kontroly a postupy související s komponentami, jako jsou operační systémy, databáze a infrastruktura.
- Průběžný monitoring účinnosti kontrol za účelem ověření, zda jsou bezpečnostní kontroly správně implementovány a nakonfigurovány.

Audity zabezpečení informací

Abychom klientům a regulačním orgánům poskytli ucelenější pohled na dodržování předpisů v oblasti bezpečnosti informací, podléhají globální technologické produkty, služby a datová centra EY auditům. Týmy EY vyžadují provedení několika auditů, například:

- Nezávislé externí audity shody s normou ISO 27001 za účelem certifikace systému řízení bezpečnosti informací používaného v našich třech globálních datových centrech v USA, Německu a Singapuru a v místních datových centrech
- Nezávislé externí audity shody s normou ISO 27017 za účelem certifikace kontrol zabezpečení informací v cloudovém výpočetním prostředí klientské technologické platformy EY Fabric
- Nezávislé externí audity shody s normou ISO 22301, které zahrnují prvky globálního systému řízení kontinuity podnikání EY
- Každoroční auditní zprávy SOC 2 (typ 2) o řídicích a kontrolních mechanismech zpracované nezávislým externím auditorem, zahrnující zásady bezpečnosti, důvěrnosti a dostupnosti a pokrývající naše tři globální datová centra v USA, Německu a Singapuru, místní datová centra, jakož i cloudovou klientskou technologickou platformu EY Fabric od externího dodavatele
- Osvědčení ISAE 3402 a SOC 1 (typ 2) pro naše tři globální datová centra v USA, Německu a Singapuru, místní datová centra, jakož i cloudovou klientskou technologickou platformu EY Fabric od třetí strany, prostřednictvím které jsou naše bezpečnostní kontroly testovány a ověřovány nezávislou třetí stranou
- Audity základních prvků, mj. technických kontrol a procesů sestavení komponent, jako jsou operační systémy, databáze a infrastruktura, prostřednictvím kterých jsou naše bezpečnostní kontroly testovány a ověřovány nezávislou třetí stranou
- Audity na místě, které zahrnují rozhovory s klíčovými členy vedení, podrobné prohlídky pracovišť, revize dokumentace a skeny zranitelností sítě. Jedná se o nejvýznamnější a nejpodrobnější formu auditu, při níž se posuzuje soulad se všemi aspekty globálních zásad společnosti EY o zabezpečení informací

Závěry auditu dodržování zásad v oblasti zabezpečení informací jsou shrnuty a prověřeny vrcholovým vedením. Následně jsou nastaveny a řízeny plány nápravných opatření.

Správa bezpečnostních výjimek

Nelze-li určitý problém vyřešit pomocí nápravných opatření, uplatní se výjimka z pravidel, kdy je cílem přezkoumat související rizika a možné alternativy. Postup udělování výjimek zahrnuje formální schvalovací proces, pravidelné ověřování jednotlivých výjimek a posouzení bezpečnostních dopadů včetně podrobného zhodnocení míry rizik. Na schválené výjimky jsou obvykle navázány kompenzační kontroly, jejichž cílem je omezit rizika, která mohou v důsledku specifických úprav nastat. Díky uvedenému procesu jsou jakékoli výjimky i případná následná nápravná opatření řádně zdokumentována, spravována a alespoň jednou ročně přezkoumána.

Shrnutí

Informace klientů EY jsou u nás v bezpečí díky integrované strategii ochrany dat a zabezpečení informací:

- U globálních aplikací a systémů posuzujeme konkrétní dopady na ochranu soukromí a podrobuje je bezpečnostním certifikacím s cílem zajistit jejich bezproblémové nasazení a provoz.
- Osobní údaje v síti EY chráníme pomocí odpovídajících fyzických, technologických a organizačních bezpečnostních opatření.
- Smlouvy uzavírané s externími zpracovateli obsahují ustanovení, jež korespondují s našimi vlastními zásadami, postupy a kontrolními mechanismy, abychom zajistili, že vaše údaje jsou spravovány řádně a v souladu s právními a regulatorními požadavky.

Klienti a jednotlivci jsou oprávněni požadovat odpovědnost jakýchkoli subjektů, které nakládají s jejich osobními údaji a důvěrnými informacemi.

Uvědomujeme si důležitost opatření souvisejících s ochranou informací a na zajištění patřičného zabezpečení informací týkajících se klientů a zaměstnanců společnosti EY vynakládáme maximální úsilí.

Máte-li dotazy nebo potřebujete-li další informace o tom, jak chráníme vás a vaše podnikání, obraťte se na zástupce společnosti EY.

EY | Building a better working world

EY přispívá k lepšímu fungování světa tím, že vytváří hodnotu pro klienty, zaměstnance, společnost i celou planetu a buduje důvěru na kapitálových trzích.

Týmy odborníků EY s využitím dat, umělé inteligence a pokročilých technologií pomáhají klientům s důvěrou a sebedůvěrou utvářet budoucnost a nacházet odpovědi na ty nejnaléhavější výzvy dneška a zítřka.

Díky detailní znalosti různých ekonomických odvětví, globálně propojené multidisciplinární síti a ekosystému nejrůznějších partnerských organizací mohou týmy našich auditorů, konzultantů, daňových poradců i odborníků na strategické a transakční poradenství poskytovat komplexní služby ve více než 150 zemích a teritoriích.

All in to shape the future with confidence.

Název EY zahrnuje celosvětovou organizaci a může zahrnovat jednu či více členských firem Ernst & Young Global Limited, z nichž každá je samostatnou právní osobou. Ernst & Young Global Limited je britská společnost s ručením omezeným garancí, která neposkytuje služby klientům.

Informace o tom, jak EY shromažďuje a používá osobní údaje, a o právech fyzických osob stanovených právními předpisy o ochraně osobních údajů jsou k dispozici na ey.com/privacy. Členské firmy EY neposkytují právní služby v zemích, kde to zákon neumožňuje. Podrobnější informace o naší organizaci najdete na našich webových stránkách ey.com.

© 2025 EYGM Limited

Všechna práva vyhrazena.

EYG no. 008242-25Gbl

2507-10837-CS

ED None

Tento materiál má pouze všeobecný informační charakter, na který není možné spoléhat jako na poskytnutí účetního, daňového, právního ani jiného odborného poradenství. V případě potřeby se prosím obraťte na svého konkrétního poradce.

ey.com