Jak zajišťujeme ochranu údajů a bezpečnost informací

Building a better working world

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 a ochrany dat

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 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 údajů

Rámec ochrany osobních údajů, jímž se společnost EY řídí, vychází ze zásad obecného nařízení EU o ochraně osobních údajů (GDPR). Řeší tak otázky, jež souvisejí s moderními nástroji a systémy pro správu dat. Ve všech členských firmách EY platí společný soubor zásad správy osobních údajů, díky němuž probíhá zpracování osobních údajů v souladu s GDPR, místními právními předpisy o ochraně osobních údajů, profesními standardy, jakož i vlastními interními zásadami jednotlivých firem. Náš rámec ochrany osobních údajů je založen na následujících principech:

- Osobní údaje chráníme prostřednictvím vhodných fyzických, technických a organizačních bezpečnostních prvků. Příslušná opatření jsou koncipována tak, aby usnadňovala dodržování požadavků na ochranu údajů již od návrhu a ze zásady standardního nastavení ochrany údajů.
- Osobní údaje zpracováváme, ukládáme a zpřístupňujeme výhradně pro legitimní obchodní účely.
- Naše smlouvy s externími zpracovateli obsahují podmínky, podle nichž musí být údaje spravovány v souladu se stejnými standardy, které sami uplatňujeme.
- Citlivým osobním údajům věnujeme zvýšenou péči.
- Stanovili jsme vhodná opatření k zachování přesnosti, úplnosti, aktuálnosti, přiměřenosti a spolehlivosti osobních údajů.
- V podobě umožňující identifikaci uchováváme osobní údaje pouze po nezbytně nutnou dobu.
- Pokud je to možné, pak jednotlivce, s nimiž členské firmy EY spolupracují, o účelu zpracování osobních údajů informujeme.
- Vedeme záznamy o zpracování osobních údajů. Zpracování, která by mohla být vysoce riziková ve vztahu k právům a svobodám fyzických osob, jsou předmětem podrobného posouzení dopadu na soukromí.

Jednotlivé složky ochrany údajů bereme vážně

Mezinárodní předávání údajů

Mezinárodní předávání osobních údajů je přísně regulováno evropským právem na ochranu osobních údajů. Země mimo Evropský hospodářský prostor, které nemají propracovanou legislativu týkající se ochrany osobních údajů, nepovažuje EU za země s dostatečnou úrovní zajištění práv jednotlivců na ochranu soukromí. Evropské právo na ochranu osobních údajů proto zakazuje předávání osobních údajů do těchto zemí; to neplatí, pokud subjekt, který informace předává, zavedl odpovídající právní záruky.

Naše týmy ustanovily závazná podniková pravidla (BCR) pro činnosti správce i pro činnosti zpracovatele jakožto mechanismus umožňující mezinárodní předávání osobních údajů mezi členskými firmami EY. BCR nám umožňují bezproblémový přenos osobních údajů v rámci členských firem EY, což usnadňuje spolupráci napříč jednotlivými servisními divizemi. Ačkoli se právní povinnosti, jež z evropského práva vyplývají, vztahují pouze na osobní údaje využívané a shromažďované v EU, aplikujeme tato závazná podniková pravidla celosvětově ve všech našich pobočkách. Kompletní znění BCR lze nalézt na internetové adrese ey.com/bcr.

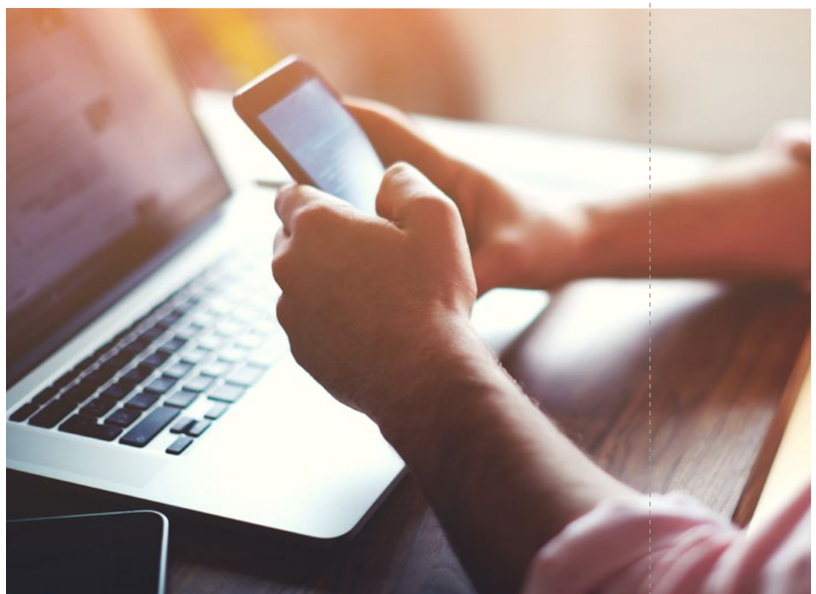
Ve smlouvách s klienty a třetími stranami v opodstatněných případech rovněž využíváme standardní smluvní doložky schválené EU.

Členská firma EY sídlící ve Spojených státech má navíc certifikaci podle tzv. „štítu soukromí“ (Privacy Shield) EU-USA a rovněž dle „štítu soukromí“ Švýcarsko-USA. Platnost štítu EU-USA na ochranu soukromí jako mechanismu pro předávání osobních údajů z EHP do USA byla Soudním dvorem Evropské unie (SDEU) zrušena. Švýcarský federální komisař pro ochranu údajů a informací rovněž dospěl k závěru, že švýcarsko-americký štít na ochranu soukromí již neposkytuje dostatečnou úroveň ochrany při předávání osobních údajů ze Švýcarska do USA. Přesto se americká členská firma zavázala zásady uvedených rámců dodržovat, ačkoliv je z hlediska legitimizace předávání osobních údajů nepovažuje za určující.

Školení a osvětové iniciativy

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 zabezpečení údajů 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.

> Sladění našich priorit v oblasti ochrany údajů a bezpečnosti informací odpovídá jednotné a soudržné vizi, kterou ve spojitosti s ochranou informací, osobních údajů a klientských dat jako organizace prosazujeme



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
- Nástroje na šifrování vyměnitelných médií
- Brány firewall na stolních počítačích a noteboocích
- Používání antivirů a software na ochranu proti malwaru
- Vícefaktorové ověřování
- Automatizovaná instalace oprav a hodnocení zranitelností zabezpečení
- Důkladné kontroly fyzického stavu, prostředí, sítí a bezpečnostního perimetru
- Technologie detekce a prevence narušení
- Monitorovací a detekční systémy

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.

Disponujeme nástroji určenými ke spolupráci s klienty EY a k bezpečnému a spolehlivému přenosu a ukládání dat.

Globální zásady společnosti EY v oblasti bezpečnosti informací

Naše zásady bezpečnosti 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.

Předepsané i doporučované politiky se týkají řady obecně uznávaných bezpečnostních požadavků, mimo jiné z následujících oblastí:

- Kontrola přístupu
- Správa majetku (klasifikace a kontrola)
- Zabezpečení komunikace a provozu
- Bezpečnost lidských zdrojů (personál)
- Pořizování, vývoj a údržba informačních systémů
- Fyzická a environmentální bezpečnost
- Hodnocení rizik

Naši odborníci dodržují příslušné profesní a odborné standardy, jakož i zásady obsažené v globálním etickém kodexu EY.

Tyto zásady jsou veřejně dostupné na globálních webových stránkách EY a představují závazné standardy, které platí celosvětově pro všechny členské firmy. Východiskem globálního etického kodexu EY je komplexní rámec chování a etiky. Má určující význam pro rozhodování všech zaměstnanců EY, bez ohledu na jejich individuální roli, pozici nebo členskou firmu. Vyžaduje, aby ctili osobní i důvěrné informace získané prostřednictvím EY, zaměstnanců i klientů společnosti nebo třetích stran, případně informace, které se daných subjektů týkají a patřičně takové údaje chránili.

Stáhnout globální etický kodex EY (PDF)

Provozní kontinuita a zotavení po havárii

Naše trvalé úsilí o ochranu firemních a klientských dat je reflektováno mimo jiné v možnostech obnovy po havárii a zajištění kontinuity provozu. Jsme odhodláni ochraňovat 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 ověřování. Mezi konkrétními metodikami zotavení po havárii a zajištění kontinuity provozních procesů figurují mimo jiné:

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

Analýza rizik dodavatelského řetězce

Pokud jde o identifikaci rizik souvisejících s dodavatelským řetězcem, řídíme se procesy hloubkové kontroly a správy dodavatelů zaměřenými na činnost třetích stran ve spojitosti s bezpečností informací, zadáváním zakázek, uzavíráním smluv, ochranou údajů a nezávislostí, včetně:

- Hodnocení potenciálních dodavatelů z hlediska souladu s našimi globálními zásadami a kontrolními mechanismy dle normy ISO 27001/2
- Due diligence včetně podrobného zhodnocení rizik a zjištění
- Opatření na snížení dopadů identifikovaných rizik
- Pomoc při výběru dodavatelů a sjednávání smluv
- K vyhodnocení inherentního a zbytkového rizika v oblasti bezpečnosti informací, dodržování předpisů a ostatních kategorií rizik, jako je přístup k datům, typ přenosu, či klasifikace a umístění dat, využíváme standardní způsoby hodnocení zabezpečení.

Bezpečnostní strategie a odpovědnost

Bez dodržování všeobecných požadavků na bezpečnost 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.

Jednotlivé složky našeho programu pro řádné zabezpečení a správu údajů důvěrné a osobní povahy mimo jiné zahrnují:

- Odpovídající zásady, standardy, pokyny a postupy řízení programu
- Důsledné kontroly zabezpečení technických aspektů
- Zajištění souladu s bezpečnostními požadavky na kontrolu, certifikaci a audit zabezpečení
- Jasně vymezená bezpečnostní strategie a definovaný plán zohledňující následující faktory:
  - Ochrana 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 zaměřený na účinnou kontrolu a nápravu incidentů, včetně pravidel týkajících se reakce na výskyt kritické zranitelnosti v systému ochrany před kybernetickými útoky

Dodržování předpisů a audity

Jako organizace disponujeme globálními programy na ochranu údajů a zabezpečení informací. Využíváme účinný řídící 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 zásadami bezpečnosti 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.

Zhodnocení dopadů 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 (DPIA). 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 DPIA vyhotoven pro všechny uživatele a správce uvedeného systému. Prováděná analýza zahrnuje také přezkum jakýchkoli přeshraničních toků údajů s ohledem na požadavky EU.

rozsáhlý soubor podnikových zásad a pokynů prosazovaných všemi našimi organizacemi 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, jež se zaměřuje na technické aspekty globálních zásad bezpečnosti informací, jako je správa záplat, zabezpečení aplikací a infrastruktury.
- Ověření provozní účinnosti, včetně přezkumu technických kontrol a procesů sestavení komponent, jako jsou operační systémy, databáze a infrastruktura.
- Průběžné sledování účinnosti bezpečnostních kontrol s cílem ověřit, zda jsou patřičně implementovány a nakonfigurovány.

Audity informační bezpečnosti

Jelikož o dodržování požadavků na bezpečnost informací chceme mít co nejúplnější přehled, podléhají naše globální technologické produkty, služby a datová centra rozličným formám auditu:

- Nezávislé audity shody s normou ISO 27001:2013 osvědčující systém řízení bezpečnosti informací používaný trojicí našich globálních datových center v USA, Německu a Singapuru a v místních data roomech.
- Každoroční auditní zprávy SOC 2 (typ 2) o řídicích a kontrolních mechanismech zpracované nezávislým externím auditorem. Rozebírají zásady bezpečnosti, důvěrnosti a dostupnosti v souvislosti s fungováním našich globálních datových center v USA, Německu a Singapuru a externí technologické cloudové platformy EY Client Technology Platform.
- Každoroční auditní zprávy ISAE 3402/SOC 1 (typ 2) nezávislého auditora, jejichž prostřednictvím jsou testovány a ověřovány bezpečnostní kontroly uplatňované v našich globálních datových centrech v USA, Německu a Singapuru, jakož i v rámci externí cloudové platformy EY Client Technology Platform.
- Kontroly zranitelnosti sítě zacílené na technické aspekty našich globálních zásad bezpečnosti informací, jako je správa záplat, zabezpečení aplikací a zabezpečení infrastruktury.
- Audity základních prvků, mj. technických kontrol a procesů sestavení komponent, jako jsou operační systémy, databáze a infrastruktura.
- Audity na místě, které zahrnují rozhovory s klíčovými vedoucími pracovníky, podrobné prohlídky pracoviště, prověrky dokumentace a kontroly zranitelnosti sítě. Jedná se o nejvýznamnější a nejpodrobnější formu auditu, při níž se posuzuje soulad se všemi aspekty globální politiky zabezpečení informací.

Zjištění vyplývající z auditů shody s předpisy v oblasti bezpečnosti informací jsou shromažďována a prověřována vrcholovým vedením. V případě potřeby jsou stanoveny a přijaty plány nápravných opatření.

Správa bezpečnostních výjimek

Nelze-li určitý problém vyřešit pomocí nápravných opatření, uplatní se výjimka z pravidel, kdy cílem je 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 zdokumentovány, spravovány a lze je v budoucnu znovu přezkoumat.

Souhrn

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

- U globálních aplikací a systémů posuzujeme konkrétní dopady na ochranu soukromí a podrobujeme je bezpečnostním certifikacím, s cílem zajistit jejich bezproblémové nasazení a provoz.
- Osobní údaje v naší síti 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 i jednotlivci právem požadují odpovědnost jakýchkoli subjektů, které nakládají s jejich osobními a důvěrnými údaji.

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 svého zástupce společnosti EY.

EY | Building a better working world

Smyslem EY je přispívat k tomu, aby svět fungoval lépe. Proto pomáháme klientům, našim zaměstnancům i širšímu společenství vytvářet dlouhodobé hodnoty a posilovat důvěru v kapitálové trhy.

Týmy odborníků EY, vybavené nejmodernějšími technologiemi, působí ve více než 150 zemích celého světa – provádějí audity a poskytují klientům širokou poradenskou podporu, která jim umožňuje růst, transformovat se a efektivně fungovat.

Naši auditoři, konzultanti, právní a daňoví poradci i odborníci na strategické a transakční poradenství si kladou ty správné otázky a dokážou najít ty správné odpovědi na složité problémy dnešního světa.

Název EY zahrnuje celosvětovou organizaci a může zahrnovat jednu či více členských firem Ernst & Young Global Limited, z nichž každá je samostatnou právnickou 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.