



Zásady ochrany osobních údajů zákazníků

Verze	Upraveno podle	Provedené změny	Datum úpravy
1.0	SPB	Obsah	02/2025

Informace o správci osobních údajů

Incode Czech Republic s.r.o., IČO: 22635891, adresa: Pujmanové 1753/10a, Nusle, 140 00 Praha 4, Česká republika ("**Incode**").

Informace o pověřenci pro ochranu osobních údajů

- Název: Data Protection Office
- Adresa: ul: Pujmanové 1753/10a, Nusle, 140 00 Praha 4, Česká republika
- E-mail: dataprotection@incode.com

Informace o příslušném dozorovém úřadu

- Název: Úřad pro ochranu osobních údajů
- Adresa: Pplk. Sochor 27, 170 00 Praha 7, Česká republika
- Tel: +420 234 665 800
- E-mail: posta@uoou.gov.cz
- Webové stránky: <http://www.uoou.cz/>

Cíle a oblast působnosti zásad ochrany údajů

Tyto zásady jsou v souladu s územní a věcnou působností nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (dále jen "**GDPR**"), zahrnují jeho základní cíle a další platné právní předpisy, jako je zákon č. 110/2019 Sb. o zpracování osobních údajů (dále jen "**český zákon o zpracování osobních údajů**").

Společnost Incode vyžaduje shromažďování a zpracování osobních údajů za účelem zákonného, řádného a komplexního výkonu své činnosti. To se týká osobních údajů zaměstnanců, klientů a návštěvníků webových stránek/platforem.

Kategorie osobních údajů, účely a důvody zpracování

Společnost Incode zpracovává různé kategorie osobních údajů různých subjektů na základě konkrétních důvodů v souladu se sledovanými cíli. V souladu s články 13 a 14 GDPR a zásadami zákonnosti, korektnosti, transparentnosti a práv subjektů údajů jsou v této části uvedeny nezbytné informace, které usnadní jednotlivcům pochopení a informovanost o jejich osobních údajích.

Kategorie osobních údajů poskytovaných subjektem údajů – fyzickou osobou jsou následující:

Údaje týkající se fyzické identity

- Jméno, druhé jméno a příjmení;
- Osobní identifikační číslo/Datum narození/Národní identifikační číslo;
- Kontakty: e-mail, adresa a telefonní číslo;
- Adresa: trvalá nebo kontaktní;
- Údaje z dokladů totožnosti (průkaz totožnosti): číslo, datum vydání a ukončení platnosti, vydávající orgán, státní příslušnost, znaky a vyobrazení;
- Biometrické údaje – fotografie/videoobraz;
- IP adresa, model mobilního zařízení a údaje o softwaru.

Údaje týkající se ekonomické identity

- Bankovní údaje: číslo bankovní karty/úctu pro platby;
- profily z platebních systémů, jako je PayPal/Epay/Revolut atd.

Kategorie osobních údajů subjektu údajů poskytnuté z jiného zdroje:

Údaje týkající se fyzické identity

- Údaje získané při úředním ověřování platnosti vašeho dokladu totožnosti z oficiálních databází příslušných orgánů státu, který doklad totožnosti vydal (pokud je přístup do těchto databází v jurisdikci státu, který doklad totožnosti vydal, možný);
- údaje získané ze strojově čitelné části nebo čipu NFC dokladu totožnosti (mohou zahrnovat fotografii z úředních databází dokladu totožnosti);
- Podpis, iniciály.

Zpracování údajů slouží k následujícím účelům, které odrážejí důvody jejich zpracování

Osobní údaje získané od subjektu – fyzické osoby budou použity pro účely poskytování našich služeb, při plnění smluvních vztahů, zákonných povinností vztahujících se na správce, jakož i pro ochranu oprávněných zájmů, a sice

- Vytvoření profilu v mobilní aplikaci správce.
- Vydávání elektronických podpisů pro fyzické osoby.
- Vydávání elektronických nebo digitálních podpisů pro vedení a zaměstnance právnických osob.
- Vydávání elektronických pečeti pro právnické osoby.
- Vydávání elektronických podpisů pro účely elektronické identifikace.

- Vytváření a vedení registrů pro účely výkaznictví.
- Finanční a účetní výkaznictví.
- Provádění úkonů na žádost subjektu údajů za účelem výkonu jeho práv podle GDPR.
- Marketingové účely.
- Výkon dalších funkcí delegovaných zákonem nebo smluvními vztahy.

Zpracování uvedených kategorií osobních údajů, které jste poskytli, je založeno na:

- Čl. 6 odst. 1 písm. c) GDPR – Dodržování právních povinností, které se vztahují na správce, včetně povinností stanovených v nařízení (EU) č. 910/2014 ("**nařízení eIDAS**") a v dalších platných právních předpisech.
- Čl. 6 odst. 1 písm. b) GDPR – Zpracování nezbytné pro plnění smlouvy, jejíž jste smluvní stranou, nebo pro přijetí opatření na vaši žádost před uzavřením smlouvy. Například stažení naší mobilní aplikace může vyžadovat určité předběžné zpracování údajů.
- Čl. 6 odst. 1 písm. f) GDPR – Zpracování nezbytné pro účely oprávněných zájmů správce, pokud nad těmito zájmy nepřevažují vaše práva a svobody. To zahrnuje zpracování pro účely přímého marketingu, přičemž je zajištěno, že máte právo kdykoli vznést námitku proti takovému zpracování.
- Čl. 6 odst. 1 písm. a) GDPR – Zpracování vašich osobních údajů pro účely přímého marketingu (např. jména a e-maily) může být založeno také na vašem svobodně uděleném, konkrétním, informovaném a jednoznačném souhlasu, pokud to vyžadují platné právní předpisy.
- Čl. 9 odst. 2 písm. a) GDPR – Zpracování vašich biometrických údajů (např. rozpoznávání obličeje a ověřování totožnosti mezi dokladem totožnosti a fotografií v reálném čase prostřednictvím mobilního zařízení) bude prováděno pouze na základě vašeho svobodně uděleného, konkrétního, informovaného a jednoznačného souhlasu.

Automatizované rozhodování pro vytvoření profilu v aplikaci "INCODE". - validate

Při využívání autentizačních služeb poskytovaných správcem je nezbytné, aby byla vaše totožnost ověřena a potvrzena prostřednictvím automatizované identifikace. Tento požadavek vyplývá z regulačních požadavků týkajících se služeb, které poskytujeme jako kvalifikovaný poskytovatel autentizačních služeb. K registraci vašeho profilu potřebujeme váš souhlas s automatizovanou identifikací prostřednictvím poskytnutí biometrických údajů (zobrazení obličeje), který by měl být svobodný, konkrétní, informovaný a jednoznačný. Informace o podmínkách a způsobech provedení identifikace naleznete v samotném prohlášení o informovaném souhlasu.

Osobní údaje se nepoužívají k neslučitelným účelům. Jejich zpracování je omezeno na účely, pro které jsou údaje shromažďovány.

Společnost Incode neshromažďuje a nezpracovává osobní údaje výhradně za účelem identifikace, která se týká:

- Odhalení rasového nebo etnického původu
- Odhalení politického, náboženského nebo filozofického přesvědčení nebo členství v odborech.
- genetické údaje, údaje týkající se sexuálního života nebo sexuální orientace.

Správce neshromažďuje a nezpracovává osobní údaje nezletilých osob.

Soubory cookie a jiné podobné technologie

Incode a naši dodavatelé mohou na webových stránkách používat soubory cookie a další podobné technologie, jako jsou pixely, tagy, webové majáky a trackery (souhrnně "soubory cookie"). Soubory cookie můžeme používat k několika účelům, včetně:

- Ukládat informace, které pomáhají Webovým stránkám správně fungovat,
- pomáhat vám s efektivnějším přístupem a navigací na Webové stránce,
- umožnit našim serverům rozpoznat vaše přihlašovací údaje a preference, abyste nemuseli při každé návštěvě Webové stránky zadávat stejné údaje,
- informovat nás o tom, jak a kdy navštěvujete a používáte naše Služby, včetně shromažďování informací o tom, které stránky na našich Webových stránkách jste si prohlíželi nebo na které odkazy jste klikali a jak jste během své návštěvy nebo během více návštěv interagovali s naším obsahem,
- Přizpůsobení vašeho prohlížení tím, že vám zobrazíme informace, které pro vás budou pravděpodobně relevantní, a
- doručování a přizpůsobování reklam a sledování reklamních kampaní.

V souvislosti s vaší aktivitou na Webových stránkách můžeme používat technologie třetích stran (například Meta Pixel a Hotjar), a to i pro reklamní účely a k analýze vašich interakcí a zkušeností s Webovými stránkami, včetně funkcí, které využíváte, způsobu navigace a vašich kliknutí/dotyků, pohybu, posouvání a stisků kláves. Tyto technologické společnosti a inzerenti mohou používat, ukládat nebo přistupovat k souborům cookie a dalším sledovacím technologiím za účelem shromažďování nebo získávání informací z Webových stránek a z jiných míst na internetu. Chcete-li změnit nastavení ochrany osobních údajů a reklamy ve službě Meta, přihlaste se ke svému účtu Meta a přejděte do nastavení svého účtu.

Můžeme také používat určité služby webové analýzy, například Google Analytics, které nám pomáhají analyzovat, jak lidé používají naše Webové stránky. Tyto informace používáme k implementaci reklamních funkcí Google, jako je dynamický remarketing, reklama založená na zájmech a hlášení demografických údajů a zájmů. Další informace

o tom, jak služba Google Analytics využívá shromážděné údaje, naleznete na adrese: google.com/policies/privacy/partners. Chcete-li se odhlásit z Google Analytics, navštivte: tools.google.com/dlpage/gaoptout. Chcete-li upravit nastavení reklamy Google, navštivte: adssettings.google.com.

Určitou reklamu založenou na zájmech můžete odhlásit pomocí nastavení prohlížeče nebo mobilního zařízení. Chcete-li se navíc odhlásit od zájmové reklamy společností, které se účastní programů Digital Advertising Alliance nebo European Interactive Digital Advertising Alliance opt-out, navštivte stránky: youradchoices.com/control a youronlinechoices.eu.

Vezměte prosím na vědomí, že my nebo jiné strany mohou při používání Webových stránek shromažďovat osobní údaje o vašich online aktivitách v průběhu času a na různých zařízeních a online webových stránkách.

Některé prohlížeče mají zabudované funkce "Do Not Track" (DNT), které mohou na navštívené webové stránky vyslat signál, že si nepřejete být sledováni. Vzhledem k tomu, že neexistuje jednotné chápání interpretace signálu DNT, naše Webové stránky v současné době na signály DNT z prohlížečů nereagují. Místo toho můžete použít řadu výše popsaných nástrojů pro kontrolu shromažďování a používání údajů.

Kategorie příjemců osobních údajů

Společnost Incode může poskytnout vaše osobní údaje třetím stranám, přičemž primárním účelem je ochrana vašich zájmů a bezpečnosti, pokud jde o plnění regulačních a smluvních povinností nebo konkrétních úkolů. Vaše osobní údaje nejsou poskytovány třetím stranám dříve, než je zajištěno, že byla přijata veškerá technická a organizační opatření k ochraně těchto údajů, a to za přísné kontroly plnění tohoto účelu. V příslušných případech dodržujeme, aby vaše údaje byly zpracovávány pouze na základě pokynů vydaných jménem správce – společnosti Incode.

Příjemci údajů mimo správce, kteří:

požadují informace na základě právního základu

- Státní a obecní úřady, agentury, instituce a další příslušné regulační orgány podle svých pravomocí (ministerstva, ředitelství, agentury, komise atd.).
- Soudní orgány (soudy, státní zastupitelství atd.).
- Regulační orgány (Úřad pro ochranu osobních údajů, Úřad pro ochranu hospodářské soutěže a další orgány dohlížející na dodržování odvětvových předpisů).
- Auditori a akreditační orgány.

- Právnícké osoby, soudní exekutoři.

Vyžadování informací na základě smlouvy

- Poskytovatelé služeb (konzultanti, odborníci, účetní, hodnotitelé, auditoři, právníci). Ke zpřístupnění údajů dochází pouze v případě oprávněného důvodu a na základě písemné dohody, aby byla zajištěna odpovídající úroveň ochrany ze strany příjemců.
- Bankovním a jiným platebním institucím za účelem úhrady dlužných částek, pokud je to nezbytné k ověření vaší totožnosti.
- Osobám pověřeným údržbou zařízení, softwaru a hardwaru používaného ke zpracování osobních údajů nezbytných pro činnost společnosti.
- Důvěryhodní partneři.

Příjemci údajů v rámci správce

- Interní sdílení mezi zaměstnanci při plném dodržení přijatých technických a organizačních opatření.

Technická a organizační opatření na ochranu údajů

Aby společnost Incode zajistila odpovídající ochranu údajů svých zaměstnanců, klientů a partnerů, zavádí všechna nezbytná organizační a technická opatření uvedená v nařízení GDPR a eIDAS, přičemž ochranu údajů zohledňuje jak ve fázi návrhu, tak standardně.

Ochrana osobních údajů ve fázi návrhu je vyjádřena vhodnými technickými a organizačními opatřeními, která společnost Incode zavedla před zahájením zpracování osobních údajů (ve fázi definování účelů a prostředků zpracování) a zajišťuje jejich uplatňování po celou dobu životního cyklu údajů. Vhodná opatření zahrnují mimo jiné šifrování údajů, zavedení funkcí automatického hlášení termínů a automatické vymazání po uplynutí doby platnosti.

Ochrana údajů je zajištěna použitím mechanismů, které standardně zaručují splnění následujících požadavků:

- Zpracovává se pouze minimální množství osobních údajů, které je nezbytně nutné k dosažení konkrétního účelu, a provádějí se provozní postupy.
- Používá se licencovaný software a certifikáty pro elektronickou ochranu systémů a internetové platformy/webové stránky/aplikace.
- Používají se šifrované e-maily s placenými soukromými doménami. Zasílání dokumentů obsahujících osobní údaje a utajované informace na e-mailové adresy s veřejnou doménou se neprovádí.
- Přístup k osobním údajům mají pouze zaměstnanci, kteří potřebují příslušné informace pro výkon svých pracovních povinností.

- Osobní údaje nejsou sdíleny s jinými zaměstnanci, pokud to není nutné k plnění jejich pracovních povinností.
- Zaměstnanci jsou povinni zacházet s údaji se zvýšenou pozorností a odpovědností po celou dobu své práce a uděleného přístupu k platformě/aplikaci. Očekává se od nich také, že nenechají svá zařízení bez dozoru.
- Dokumenty související se zpracováním osobních údajů subjektů se neukládají v kanceláři společnosti. Informace jsou zcela digitální a ukládají se v cloudových systémech, přičemž se řídí zásadami poskytovatelů cloudových služeb. Existuje zákonná povinnost uchovávat některé dokumenty obsahující osobní údaje v papírové podobě, což se děje ve speciálně určené skříni s uzamykacím mechanismem.
- Připojení ke cloudovým službám probíhá prostřednictvím přístupového kanálu HTTPS a každý zaměstnanec společnosti je seznámen se zásadami počítačové a informační bezpečnosti. Při aktualizaci těchto zásad je každý příslušný zaměstnanec o změnách informován.
- Pro naše interní operace a zpracování dat klientů používáme cloudové platformy, které poskytují vzdálený přístup s oprávněními na úrovni uživatelů a přísnými zásadami zabezpečení dat.
- Přístup k datům je udělován konkrétním zaměstnancům prostřednictvím individuálních pracovních účtů pro provádění konkrétních úkolů.
- Po uvolnění ze svých povinností ztrácí jednotlivec okamžitý přístup ke všem souvisejícím datům.
- Byla stanovena politika vytváření hesel a uživatelských práv.
- Zaměstnanci procházejí školením pro správné dodržování GDPR a uplatňování zavedených technických a organizačních opatření a postupů.
- Údaje jsou uchovávány po minimální dobu nezbytnou k dosažení účelů zpracování a po uplynutí této doby jsou vymazány podle příslušných pravidel a postupů.
- Údaje, jejichž účel shromažďování pominul, jsou nevratně zničeny protokolem o vymazání.
- Jakýkoli přístup k údajům, jejich předávání nebo sdílení je přípustné pouze tehdy, pokud existuje platný právní základ (např. smlouva, souhlas subjektu údajů nebo naše právní povinnosti).
- Sdílení a stahování jakýchkoli údajů nebo důvěrných informací, k nimž mají zaměstnanci přístup v rámci svých pracovních povinností, je přísně zakázáno. Ukládání takových údajů na osobní zařízení (mimo jiné včetně notebooků, tabletů, mobilních zařízení, fotoaparátů nebo chytrých telefonů) nebo zaznamenávání takových údajů v jakékoli formě (např. pořizováním fotografií, videí, snímků obrazovky nebo jiných obrázků) je rovněž zakázáno.

- V souladu s čl. 8 odst. 2 písm. v) nařízení GDPR je zavedena nejvyšší úroveň zabezpečení informací a hardwaru, aby byly splněny požadavky článku 19 nařízení GDPR.
- Nepřetržitá údržba systému probíhá 24 hodin denně, 7 dní v týdnu, aby se minimalizovala možnost narušení bezpečnosti, úniku informací a krádeže identity.
- Každých 12 měsíců se provádí kompletní interní audit a kontrola systému.
- V případě narušení bezpečnosti je služba cílové osobě (cílovým osobám) dočasně nebo trvale pozastavena, aby se zabránilo neoprávněnému jednání třetích stran.
- Správce přijímá nezbytná opatření, aby zajistil, že zpracovatel údajů a jakákoli fyzická osoba, která jedná z pověření správce, zpracovávají tyto údaje pouze na základě pokynu správce pro příslušný účel.
- V případě, že dojde k porušení zabezpečení osobních údajů, správce po zjištění této skutečnosti informuje příslušný dozorový úřad a v případě potřeby i subjekt údajů, kterého se škodlivé jednání týká.

Společnost Incode má možnost, pokud je to nutné z bezpečnostních důvodů, zavést další klíč pro ochranu. Pro zajištění maximální bezpečnosti při zpracování, přenosu a ukládání údajů můžeme použít další ochranné mechanismy.

Předávání údajů do třetích zemí

Předávání osobních údajů do třetích zemí se neprovádí a zpracování osobních údajů mimo rámec Evropské unie neprobíhá.

Doba uchovávání údajů

Společnost Incode obvykle ukončí úplné zpracování osobních údajů pro uvedené účely po ukončení smluvních vztahů nebo na žádost subjektu údajů. Údaje však nejsou vymazány před uplynutím zákonem stanovených povinností pro uchovávání údajů, a to v souladu se zásadou omezeného uchovávání. Vaše osobní údaje nebudou vymazány nebo anonymizovány, pokud je to nezbytné pro probíhající soudní, správní řízení nebo řízení o stížnosti. Údaje jsou uchovávány po dobu nepřesahující nezbytně nutnou. Níže jsou uvedeny doby uchovávání údajů pro kategorie údajů zvláštního významu.

Zákonem definované doby uchovávání údajů:

- Informace obsažené v rejstříku podle článků 24 a 28 nařízení eIDAS - 10 let, včetně doby po ukončení činnosti,
- Údaje zpracováváné na základě souhlasu subjektu údajů, s výjimkou biometrických údajů - do odvolání souhlasu;
- Údaje zpracováváné za účelem plnění našich právních povinností podle platných právních předpisů budou uchovávány po dobu nezbytnou k plnění těchto povinností (až 10 let);

- Uchovávání a zpracování účetních údajů - 10 let od roku následujícího po poslední platbě,

doby uchovávání definované správcem:

- Biometrické údaje zpracovávané při identifikaci subjektu údajů v procesu registrace a aktivace Aplikace - až 5 minut od procesu identifikace;
- Údaje a záznamy obsažené v logovacích souborech shromážděné během neúspěšné identifikace a/nebo ukončených procesů registrace subjektu údajů a aktivace Aplikace - do 2 let od výskytu.

Hlášení bezpečnostních incidentů

Společnost Incode zavedla strukturovaný systém hlášení bezpečnostních incidentů. V případě jakéhokoli narušení bezpečnosti údajů postupuje společnost Incode plně v souladu s GDPR, aby minimalizovala případné škody. V případě potřeby neprodleně a ve stanovené lhůtě informuje Úřad pro ochranu osobních údajů.

Pokud je pravděpodobné, že porušení povede k vysokému riziku pro práva a svobody fyzických osob, informujeme bez zbytečného odkladu také dotčené subjekty údajů.

Reakce na incident zahrnuje:

- identifikaci a zamezení narušení;
- posouzení dopadu a úrovně rizika;
- provedení nápravných opatření, aby se zabránilo opakování;
- zdokumentování všech incidentů a nápravných opatření.

Všechny bezpečnostní incidenty jsou interně zaznamenávány a naše postupy reakce jsou pravidelně revidovány, aby bylo zajištěno trvalé dodržování předpisů a ochrana údajů.

Práva subjektů údajů - pro fyzické osoby

Právo na informace a přístup.

Máte právo požádat o:

- *Informace* o tom, zda jsou údaje, které se vás týkají, zpracovávány, o účelech takového zpracování, o kategoriích údajů a o příjemcích nebo kategoriích příjemců, kterým jsou údaje zpřístupněny;
- *sdělení* ve srozumitelné formě obsahující zpracovávané osobní údaje a veškeré dostupné informace o jejich zdroji;
- *Informace* o logice, která stojí za jakýmkoli automatizovaným zpracováním osobních údajů, které se vás týkají, alespoň v případech automatizovaného rozhodování.

Právo na opravu.

V případech, kdy zpracováváme neúplné nebo nesprávné údaje, máte právo kdykoli požádat o jejich opravu:

- vymazání, opravu nebo zablokování vašich osobních údajů, jejichž zpracování není v souladu s právními požadavky;
- informovat třetí strany, kterým byly vaše osobní údaje zpřístupněny, o vymazání, opravě nebo zablokování, s výjimkou případů, kdy to není možné nebo vyžaduje nadměrné úsilí.

Právo na výmaz.

Právo na výmaz neboli "právo být zapomenut" poskytuje možnost v případě, že si nepřejete, aby byly vaše údaje dále zpracovávány, a neexistuje žádný právní základ pro jejich uchovávání, požádat o jejich výmaz na základě jednoho z následujících důvodů:

- Osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
- odvoláte svůj souhlas, na němž je zpracování údajů založeno;
- vznesete námitku proti zpracování a neexistuje žádný převažující právní základ pro pokračování zpracování;
- Osobní údaje byly zpracovány protiprávně;
- Osobní údaje musí být vymazány, aby byla splněna právní povinnost;

"Právo být zapomenut" není absolutním právem. Existují situace, kdy správce může odmítnout výmaz údajů, a to v případě, že zpracování konkrétních údajů je nezbytné pro některý z následujících účelů:

- Výkon práva na svobodu projevu a informací.
- Archivace pro účely ve veřejném zájmu, vědecký výzkum, historický výzkum nebo statistické účely.
- Stanovení, výkon nebo obhajoba právních nároků.

Právo vznést námitku.

Kdykoli máte právo vznést námitku proti zpracování vašich osobních údajů, pokud k tomu existuje právní základ. Je-li námitka oprávněná, nelze osobní údaje příslušné osoby dále zpracovávat.

Právo na omezení zpracování.

O omezení zpracování osobních údajů můžete požádat, pokud:

- popíráte přesnost údajů po dobu, po kterou je jejich přesnost ověřována, nebo
- Zpracování údajů je bez právního základu, ale namísto výmazu si přejete jejich omezené zpracování; nebo
- Tyto údaje již nepotřebujeme (pro konkrétní účel), ale vy je potřebujete k určení, uplatnění nebo obhajobě právních nároků; nebo
- Vznesli jste námitku proti zpracování údajů a čekáte, až správce ověří zákonnost důvodů.

Právo na přenositelnost údajů.

Můžete nás požádat o poskytnutí osobních údajů, které jste nám svěřili, v uspořádaném, strukturovaném, běžně používaném a strojově čitelném formátu jinému správci, pokud

- údaje zpracováváme na základě smlouvy a prohlášení o souhlasu, který lze odvolat, nebo na základě smluvních závazků, a
- Zpracování se provádí automaticky.

Právo na odvolání souhlasu.

Máte právo kdykoli odvolat svůj souhlas se zpracováním osobních údajů, pokud je zpracování založeno na vašem souhlasu. Takové odvolání nemá vliv na zákonnost zpracování založeného na souhlasu před jeho odvoláním.

Právo na podání stížnosti.

Pokud se domníváte, že porušujeme platné předpisy, obraťte se na nás, abychom věc objasnili. Samozřejmě máte právo podat stížnost u příslušného úřadu. Dozorovým úřadem v České republice je Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (<http://www.uoou.cz/>).

Právo na náhradu škody.

Podle § 39 českého zákona o zpracování osobních údajů a čl. 82 odst. 1 GDPR má každý, kdo utrpěl škodu v důsledku porušení ustanovení GDPR nebo jiných platných právních předpisů o ochraně osobních údajů, právo získat náhradu škody prostřednictvím žaloby u příslušného soudního orgánu.

Uplatnění vašich práv

Žádosti o uplatnění svých práv zasílejte na jednu z následujících e-mailových adres: dataprotection@incode.com.

Měly by být podepsány kvalifikovaným elektronickým podpisem (QES) nebo jiným způsobem, který nesporně ověřuje vůli osoby, která žádost podává. Na vaši žádost odpovíme do jednoho měsíce od jejího podání. Pokud je objektivně nutná delší lhůta, například pro shromáždění všech požadovaných údajů, nebo pokud to výrazně ztěžuje naši činnost, může být tato lhůta prodloužena až o 30 dnů. V našem rozhodnutí přístup a/nebo požadované informace povolíme nebo zamítneme, přičemž vždy poskytneme odůvodněnou odpověď.

Minimální informace obsažené v žádosti by měly být následující: jméno, kontaktní údaje, popis žádosti a podpis. Pokud je žádost podávána jménem jiné osoby, může být vyžadována plná moc nebo jiný doklad o oprávnění.

Pokud jde o výše uvedená práva: na informace, na opravu, "právo být zapomenut", vznést námitku, na omezení zpracování, nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, odvolat souhlas, podat stížnost, a s ohledem na úkony správce v souvislosti s těmito právy je vytvořen zvláštní rejstřík pro evidenci všech provedených úkonů.

Prvotní poskytnutí odpovědi na podanou žádost je bezplatné. V případech nadbytečnosti (opakování - více než 2/ dvě/ žádosti stejného obsahu v období 12/ dvanácti/ měsíců) nebo zjevné neopodstatněnosti žádostí téhož subjektu může správce požadovat přiměřený poplatek za vyřízení žádosti nebo odmítnout žádost vyřídit.

Zásady zpracování osobních údajů v souladu s GDPR

- "Zákonnost, korektnost a transparentnost" - Vaše údaje jsou zpracovávány v souladu s platnými právními předpisy, korektně a transparentně vůči subjektu údajů.
- "Omezení účelu" - Vaše údaje jsou shromažďovány pro konkrétní, výslovně uvedené a legitimní účely a nejsou dále zpracovávány způsobem, který je s těmito účely neslučitelný.
- "Minimalizace údajů" - Typy údajů, které shromažďujeme, jsou vhodné, související a omezené na nezbytné minimum v souvislosti s účely, pro které jsou osobní údaje zpracovávány.
- "Přesnost" - Přesné a v případě potřeby aktualizované, přičemž je třeba přijmout veškerá přiměřená opatření k zajištění včasného výmazu nebo opravy nepřesných osobních údajů s ohledem na účely, pro které jsou zpracovávány.
- "Omezení uchovávání" - Vaše údaje jsou uchovávány ve formě, která umožňuje identifikaci subjektu údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou osobní údaje zpracovávány.
- "Integrita a důvěrnost" - Zpracovávány způsobem, který zajišťuje odpovídající úroveň zabezpečení osobních údajů, včetně ochrany před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, a to za použití vhodných technických nebo organizačních opatření.

Definice

Termín	Definice
Osobní údaje	Jakákoli informace týkající se identifikované nebo identifikovatelné fyzické osoby.
Subjekt údajů	fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména prostřednictvím identifikátoru, jako je jméno, identifikační číslo, lokalizační údaje, online identifikátor nebo jeden či více faktorů specifických pro fyzickou, fyziologickou, genetickou, duševní, ekonomickou, kulturní nebo sociální identitu této fyzické osoby.
Zpracování	jakákoli operace nebo soubor operací prováděných s osobními údaji nebo soubory osobních údajů, ať již automatizovaně či nikoli, jako je shromažďování, zaznamenávání, uspořádávání, strukturování, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, zpřístupňování přenosem, šíření nebo jiné zpřístupňování, seřazování nebo kombinování, omezování, výmaz nebo zničení.
Omezení zpracování	Označení uložených osobních údajů s cílem omezit jejich zpracování v budoucnu.
Pseudonymizace	Zpracování osobních údajů takovým způsobem, že údaje již nelze přiřadit konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a podléhají technickým a organizačním opatřením, která zajistí, že osobní údaje nebudou přiřazeny identifikované nebo identifikovatelné fyzické osobě.
Správce	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky

	zpracování osobních údajů. Pokud jsou účely a prostředky takového zpracování určeny právem Unie nebo členského státu, může být správce nebo konkrétní kritéria pro jeho jmenování stanovena právem Unie nebo členského státu.
Zpracovatel	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje jménem správce.
Souhlas subjektu údajů	jakýkoli svobodně daný, konkrétní, informovaný a jednoznačný projev vůle subjektu údajů, který prohlášením nebo jasným potvrzujícím úkonem vyjadřuje souhlas se zpracováním osobních údajů, které se ho týkají.
Profilování	jakákoli forma automatizovaného zpracování osobních údajů spočívající v použití těchto údajů k vyhodnocení určitých osobních aspektů týkajících se fyzické osoby, zejména k analýze nebo předvídání aspektů týkajících se pracovního výkonu, ekonomické situace, zdraví, osobních preferencí, zájmů, spolehlivosti, chování, polohy nebo pohybu této fyzické osoby.
Automatizované rozhodování	schopnost rozhodovat pomocí technologických prostředků bez zásahu člověka.
Elektronická identifikace	proces používání údajů v elektronické podobě pro identifikaci fyzických osob, které jednoznačně reprezentují fyzickou nebo právnickou osobu nebo fyzickou osobu zastupující právnickou osobu.
Důvěryhodné strany	příjemci kvalifikovaných elektronických podpisů (QES), například jako součást elektronických výpisů, které se spoléhají na ověřování pravosti a/nebo elektronické podpisy ověřené veřejným klíčem tohoto certifikátu.
Porušení ochrany osobních údajů	Porušení zabezpečení vedoucí k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému

	zveřejnění nebo přístupu k osobním údajům, které jsou přenášeny, uchovávány nebo jinak zpracovávány.
Příjemce	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterému jsou osobní údaje zpřístupněny, ať už se jedná o třetí stranu, nebo ne. Za příjemce se nepovažují orgány veřejné moci, které mohou získat osobní údaje v rámci konkrétního šetření v souladu s právem Unie nebo členského státu. Zpracování těchto údajů těmito orgány veřejné moci je v souladu s platnými pravidly ochrany údajů podle účelu zpracování.
Třetí země	Jakýkoli stát, který není členem Evropské unie nebo smluvní stranou Dohody o Evropském hospodářském prostoru.

Incode PSC