DOTYKAČKA

Dotykačka ČR s.r.o.
Plzeňská 3217/16
150 00 Praha 5 – Smíchov
IČ: 06290914

Zpracování osobních údajů v souladu s požadavky EU GDPR

OBECNÁ POLITIKA OCHRANY OSOBNÍCH ÚDAJŮ

Ev. značka	01.1 EU GDPR
Verze	1.1
Datum verze	05/05/2018
Vypracoval	Ing. Petr Krůček
Schválil	
Klasifikace	PRO VNITŘNÍ POTŘEBU

PLATNÉ OD: 25/05/2018

Petr Menclík
Ředitel společnosti

Historie verzí

Datum	Verze	Vypracoval	Popis změn
05/05/2018	1.0	Ing. Petr Krůček	Nový dokument
7.1.2019	1.1	Ing. Ondřej Bohuslav	Úprava seznamu zpracovatelů

Obsah

1 Účel, rozsah, uživatelé

Dotykačka ČR s.r.o., dále jen "Organizace", usiluje o dodržování platných zákonů a předpisů týkajících se ochrany osobních údajů v zemích, kde Organizace působí. Tato politika stanoví základní principy, kterými Organizace zpracovává osobní údaje spotřebitelů, zákazníků, dodavatelů, obchodních partnerů, zaměstnanců a dalších osob, a uvádí odpovědnost svých útvarů a zaměstnanců při zpracování osobních údajů.

Tato politika se vztahuje na Organizaci a její přímo či nepřímo řízené dceřiné organizace, které vykonávají činnost v rámci Evropského hospodářského prostoru (EHP) nebo zpracovávají osobní údaje subjektů údajů v EHP.

UŽIVATELÉ TOHOTO DOKUMENTU JSOU VŠICHNI ZAMĚSTNANCI A VŠICHNI DODAVATELÉ, KTEŘÍ PRACUJÍ VE PROSPĚCH ORGANIZACE.

2 Referenční dokumenty

- EU GDPR 2016/679 (nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a zrušení směrnice 95/46 / ES)
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. července 2017
- Pokyny pracovní skupiny WP29
- Politika ochrany osobních údajů zaměstnanců
- Politika uchování osobních údajů
- Popis role pověřence pro ochranu osobních údajů
- Pokyny pro inventarizaci činností zpracování
- Postup při podání žádosti subjektu údajů o přístup k údajům
- Metodika posouzení vlivu na ochranu osobních údajů
- Bezpečnostní politika IT
- Postup při porušení zabezpečení osobních údajů a oznámení

3 Definice pojmů a terminologie

Následující definice pojmů používaných v tomto dokumentu vycházejí z článku 4 nařízení EU GDPR:

GDPR – nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46 / ES (General Data Protection Regulation – obecné nařízení o ochraně údajů).

Subjekt údajů: identifikovaná nebo identifikovatelná fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor. Jedná se o zaměstnance, klienty, dodavatele, obchodní partnery, občany města a další osoby.

Osobní údaje: veškeré informace o subjektu údajů, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor, nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Zvláštní kategorie osobních údajů / citlivé osobní údaje: osobní údaje, které jsou svým charakterem obzvláště citlivé ve vztahu k základním právům a svobodám, vyžadují zvláštní ochranu, neboť jejich zpracování by mohlo představovat významná rizika pro základní práva a svobody. Tyto osobní údaje zahrnují osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, obsahují genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

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.

Zpracovatel: fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Posouzení vlivu na ochranu údajů (DPIA): proces určený k popisu činností zpracování, posuzování nezbytnosti a přiměřenosti zpracování a k podpoře řízení rizik pro práva a svobody fyzických osob vyplývající ze zpracování osobních údajů.

Zpracování: jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Anonymizace: proces nevratně de-identifikující osobní údaje tak, že osoba nemůže být identifikována v rámci přiměřené doby, nákladů a technologií buď správcem, nebo jakoukoli jinou osobou. Zásady zpracování osobních údajů se nevztahují na anonymní údaje, protože již nejsou osobními údaji.

Pseudonymizace: zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

Dozorový úřad: nezávislý orgán veřejné moci zřízený členským státem podle článku 51, v České republice jím je Úřad pro ochranu osobních údajů.

Třetí strana: fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.

Žádost subjektu údajů o přístup k údajům (DSAR): žádost podaná fyzickou osobou nebo právním zástupcem fyzické osoby o přístup k informacím, které Organizace o této osobě uchovává. Žádost subjektu údajů o přístup k osobním údajům poskytne subjektům údajů právo nahlížet vlastní osobní údaje, stejně jako požadovat kopie těchto osobních údajů.

Posouzení vlivu na ochranu údajů (DPIA): proces určený k popisu činností zpracování, posuzování nezbytnosti a přiměřenosti zpracování a k podpoře řízení rizik pro práva a svobody fyzických osob vyplývající ze zpracování osobních údajů.

Porušení zabezpečení osobních údajů: porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

4 Základní principy týkající se zpracování osobních údajů

Zásady ochrany osobních údajů popisují základní odpovědnosti organizací, zpracovávají osobní údaje. V čl. 5 odst. 2 GDPR se stanoví, že "správce odpovídá za dodržování zásad a musí být schopen toto dodržení souladu doložit."

4.1 Zákonnost, korektnost a transparentnost

Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány zákonným způsobem, transparentně a korektně.

4.2 Účelové omezení

Osobní údaje musí být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.

4.3 Minimalizace osobních údajů

Osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. Organizace musí anonymizovat nebo pseudonymizovat osobní údaje, pokud je to možné, a snížit tak rizika pro dotčené subjekty údajů.

4.4 Přesnost

Osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.

4.5 Omezení uložení

Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány.

4.6 Integrita a důvěrnost

Osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením

4.7 Odpovědnost

Správci osobních údajů odpovídají a musí být schopni doložit soulad s výše uvedenými zásadami.

5 Ochrana osobních údajů v hlavních aktivitách

S cílem prokázat soulad se zásadami ochrany osobních údajů by měla organizace začlenit ochranu osobních údajů do svých podnikatelských činností.

5.1 Oznámení subjektu údajů

Vizte 6 Pokyny pro správné zpracování

5.2 Možnost volby a souhlas subjektu údajů

Vizte 6 Pokyny pro správné zpracování

5.3 Shromažďování

Organizace se musí snažit shromáždit co nejmenší množství osobních údajů. Pokud jsou osobní údaje shromažďovány od třetí strany, ředitel společnosti musí zajistit, aby byly osobní údaje shromažďovány a zpracovávány zákonně.

5.4 Používání, uchovávání a likvidace

Účely, metody, omezení ukládání a doba uchovávání osobních údajů musí být v souladu s informacemi obsaženými v oznámení o ochraně osobních údajů.

Organizace musí zachovat přesnost, integritu, důvěrnost a relevanci osobních údajů na základě účelu zpracování. Aby se zabránilo odcizení, chybnému použití nebo zneužívání osobních údajů a zabránilo porušení zabezpečení osobních údajů, musí být použita přiměřená bezpečnostní opatření určená k ochraně osobních údajů. Vedoucí oddělení IT odpovídá za splnění požadavků uvedených v této části.

5.5 Předání třetím stranám

Ve všech případech, kdy Organizace používá třetí stranu – dodavatele nebo obchodního partnera – ke zpracování osobních údajů v zastoupení (zpracovatele), musí vedoucí oddělení IT zajistit, aby tento zpracovatel poskytl informace o opatřeních k ochraně osobních údajů odpovídající souvisejícím rizikům.

Organizace musí od zpracovatele smluvně požadovat, aby poskytl náležitou úroveň ochrany osobních údajů. Dodavatel nebo obchodní partner musí zpracovávat osobní údaje pouze za účelem plnění svých smluvních závazků vůči Organizaci nebo na základě pokynů Organizace, a nikoliv pro jiné účely. Pokud Organizace zpracovává osobní údaje společně s nezávislými třetími stranami, musí Organizace výslovně uvést své povinnosti a povinnosti třetí strany v příslušné smlouvě nebo jiném právně závazném dokumentu, například ve smlouvě o zpracování osobních údajů.

5.6 Přeshraniční přenos osobních údajů

Před přenosem osobních údajů z Evropského hospodářského prostoru (EHP) musí být použita přiměřená ochranná opatření včetně podpisu „doložky pro přeshraniční předávání osobních údajů“, jak požaduje Evropská unie. V případě potřeby musí být získána povolení příslušného dozorového úřadu (v ČR Úřad pro ochranu osobních údajů). Subjekt, který přijímá osobní údaje (dovozce údajů), musí dodržovat zásady zpracování osobních údajů stanovené v „Postupu pro přeshraniční předávání osobních údajů“.

5.7 Práva přístupu subjektu údajů

Při výkonu funkce správce osobních údajů je vedoucí oddělení IT zodpovědný za to, aby subjekty údajů měly k dispozici přiměřený mechanismus umožňující přístup k jejich osobním údajům, který jim musí umožnit aktualizovat, opravit, vymazat nebo předávat jejich osobní údaje. Přístupový mechanismus je podrobněji popsán v dokumentu „Postup při podání žádosti subjektu údajů o přístup k údajům.“

5.8 Přenositelnost osobních údajů

Subjekty údajů mají právo zdarma obdržet na vyžádání kopii dat, které správci poskytli, a to ve strukturovaném formátu a předat tyto údaje jinému správci. Vedoucí oddělení IT odpovídá za to, že tyto žádosti budou zpracovány do jednoho měsíce, nebudou nepřiměřené a neovlivní práva na osobní údaje jiných osob.

5.9 Právo být zapomenut

Subjekty údajů mají na požádání právo na vymazáni svých osobních údajů. Pokud Organizace vystupuje jako správce, musí vedoucí oddělení IT přijmout nezbytná opatření (včetně technických opatření) k informování třetích stran, které tyto údaje používají nebo zpracovávají, k provedení (vyhovění) žádosti.

Nevyhovět takové žádosti lze jen v taxativně vymezených případech, které stanoví čl. 17 odst. 3 obecného nařízení GDPR, zejména jedná-li se o zpracování osobních údajů pro splnění právní povinnosti, nebo pro splnění úkolu provedeného ve veřejném zájmu, nebo při výkonu veřejné moci.

6 Pokyny pro správné zpracování

Osobní údaje smí být zpracovávány pouze tehdy, je-li výslovně povoleno ředitelem společnosti.

Organizace musí rozhodnout, zda má provádět posouzení vlivu na ochranu osobních údajů pro každou činnost zpracování osobních údajů podle pokynů pro posuzování vlivu na ochranu osobních údajů.

6.1 Oznámení subjektu údajů

V době shromažďování nebo před shromažďováním osobních údajů pro jakýkoli druh činností zpracování, je vedoucí oddělení IT zodpovědný za řádné informování subjektů údajů o:

- kategoriích zpracovávaných osobních údajů,
- účelu zpracování,
- právech subjektů údajů s ohledem na jejich osobní údaje,
- době uchovávání,
- případných přeshraničních přenosech osobních údajů,
- sdílení osobních údajů s třetími stranami a
- bezpečnostních opatřeních Organizace na ochranu osobních údajů.

Tyto informace jsou poskytovány prostřednictvím Oznámení o zpracování osobních údajů.

Pro každou činnost zpracování musí existovat relevantní Oznámení o zpracování osobních údajů, které zohlední konkrétní činnost a kategorii zpracování osobních údajů.

Pokud jsou osobní údaje předávány do třetí země v souladu se zásadami přeshraničního předávání osobních údajů, mělo by toto upozornění odrážet a jasně uvádět, jaké osobní údaje jsou přenášeny a kam.

Pokud jsou shromažďovány zvláštní kategorie osobních údajů (citlivé osobní údaje), musí pověřenec pro ochranu osobních údajů zajistit, aby oznámení o ochraně osobních údajů výslovně uvádělo účel, pro který jsou tyto citlivé osobní údaje shromažďovány.

6.2 Získání souhlasu

Organizace může zpracovávat osobní údaje subjektů údajů pro své legitimní účely a tam, kde je to možné primárně využívá ostatní zákonné tituly, odlišné od získání souhlasu subjektu údajů.

Kdykoli je zpracování osobních údajů založeno na souhlasu subjektu údajů, je za uchovávání záznamu o poskytnutém souhlasu odpovědný vedoucí oddělení IT. Vedoucí oddělení IT je zodpovědný za to, že subjekty údajů mají možnost poskytnout souhlas a musí je také informovat a zajistit, že jejich souhlas (kdykoli je souhlas používán jako zákonný důvod pro zpracování) může být kdykoli odvolán.

Pokud jde o shromažďování osobních údajů osob mladších 15 let, vedoucí oddělení IT musí zajistit, aby byl souhlas vyjádřen nebo schválen rodičem / zástupcem / zákonným zástupcem. Souhlas musí být udělen před shromážděním osobních údajů.

Při žádostech o opravu, změnu nebo zničení záznamů osobních údajů musí vedoucí oddělení IT zajistit, aby tyto žádosti byly zpracovány v přiměřeném časovém rámci 30 dnů. Vedoucí oddělení IT musí také musí žádosti evidovat a uchovat je.

Osobní údaje musí být zpracovávány pouze pro účely, pro které byly původně shromážděny. V případě, že Organizace chce zpracovávat shromážděné osobní údaje pro jiný účel, musí usilovat o souhlas subjektů údajů v jasném a stručném sdělení. Každá taková žádost by měla obsahovat původní účel, pro který byly osobní údaje shromážděny, a také nový nebo doplňující účel nebo účely. Žádost musí obsahovat také důvod změny účelu nebo účelů. Pověřenec pro ochranu osobních údajů odpovídá za dodržování pravidel uvedených v tomto odstavci.

Nyní a v budoucnu musí vedoucí oddělení IT zajistit, aby metody shromažďování osobních údajů byly v souladu s příslušnými právními předpisy, osvědčenými postupy a oborovými standardy.

Vedoucí oddělení IT je odpovědný za vytvoření a vedení registru oznámení o ochraně osobních údajů.

7 Organizace a odpovědnost

Odpovědnost za zajištění odpovídajícího zpracování osobních údajů nese každý, kdo pro Organizaci pracuje nebo má přístup k osobním údajům zpracovávaných Organizací.

Klíčové oblasti odpovědnosti za zpracování osobních údajů spočívají v následujících organizačních rolích:

Představenstvo nebo jiný příslušný **rozhodovací orgán** rozhoduje a schvaluje obecné strategie Organizace týkající se ochrany osobních údajů.

Pověřenec pro ochranu osobních údajů (DPO) nebo jiný příslušný zaměstnanec, který je pověřen řízením programu ochrany osobních údajů, odpovídá za vývoj a údržbu politik ochrany osobních údajů a další činnosti tak, jak je definováno v popisu pracovní pozice pověřence pro ochranu osobních údajů.

Útvar zajišťující **právní služby**, případně včetně externího právního poradenství, spolu s pověřencem pro ochranu osobních údajů sleduje a analyzuje související zákony a předpisy, rozvíjí požadavky na dodržování předpisů a pomáhá ostatním útvarům při dosahování cílů týkajících se osobních údajů.

Vedoucí oddělení IT zodpovídá za:

- Zajištění, aby všechny systémy, služby a zařízení používané pro ukládání osobních údajů splňovaly přijatelné bezpečnostní standardy.
- Provádění pravidelných kontrola a monitorování, aby bylo zajištěno, že bezpečnostní opatření, hardware a software pracují správně.

Marketingový ředitel zodpovídá za:

- Schválení všech prohlášení o ochraně osobních údajů připojených ke komunikaci, jako jsou e-maily a dopisy.
- Řešení dotazů na ochranu osobních údajů od novinářů nebo médií.
- V případě potřeby spolupracuje s pověřencem pro ochranu osobních údajů, aby bylo zajištěno, že marketingové aktivity budou ve shodě s politikami ochrany osobních údajů.

Vedoucí oddělení HR je zodpovědný za:

- Zlepšení povědomí zaměstnanců o ochraně osobních údajů.
- Zvyšování odborných znalostí o ochraně osobních údajů a vzdělávání pro zaměstnance pracující s osobními údaji.
- Ochranu osobních údajů zaměstnanců. Musí zajistit, aby osobní údaje zaměstnanců byly zpracovávány na základě legitimních účelů a potřeb zaměstnavatele.

Vedoucí oddělení BO je zodpovědný za přenos odpovědností na ochranu osobních údajů dodavatelům a zlepšování úrovně informovanosti dodavatelů o ochraně osobních údajů, jakož i snižování požadavků na osobní údaje od třetích stran. Útvar nákupu musí zajistit, aby si Organizace vyhradila právo auditu dodavatelů / zpracovatelů.

8 Reakce na případy porušování osobních údajů

Pokud se Organizace zaznamená podezření na porušení zabezpečení osobních údajů, Vedoucí oddělení IT musí provést interní šetření a včas přijmout vhodná nápravná opatření v souladu s Postupem při porušení zabezpečení osobních údajů a oznámení. V případě jakéhokoli rizika týkajícího se práv a svobod subjektů údajů musí Organizace bez zbytečného odkladu a pokud možno do 72 hodin oznámit poručení osobních údajů příslušným orgánům pro ochranu osobních údajů.

9 Správa záznamů vedených na základě tohoto dokumentu

Název záznamu	Místo uložení	Osoba odpovědná za správu úložiště	Opatření pro ochranu záznamu	Doba uchování
Formulář souhlasu subjektu údajů se zpracováním	Intranet Organizace a konkrétní adresář	Vedoucí oddělení IT	K souboru mohou přistupovat pouze oprávněné osoby	10 let
Formulář odvolání souhlasu subjektu údajů se zpracováním	Intranet Organizace a konkrétní adresář	Vedoucí oddělení IT	K souboru mohou přistupovat pouze oprávněné osoby	10 let
Formulář rodičovského souhlasu	Intranet Organizace a konkrétní adresář	Vedoucí oddělení IT	K souboru mohou přistupovat pouze oprávněné osoby	10 let
Formulář odvolání rodičovského souhlasu	Intranet Organizace a konkrétní adresář	Vedoucí oddělení IT	K souboru mohou přistupovat pouze oprávněné osoby	10 let
Obecné oznámení o zpracování osobních údajů	Intranet Organizace a konkrétní adresář	Vedoucí oddělení IT	K souboru mohou přistupovat pouze oprávněné osoby	5 let po expiraci
Registr oznámení o zpracování osobních údajů	Intranet Organizace a konkrétní adresář	Vedoucí oddělení IT	K souboru mohou přistupovat pouze oprávněné osoby	Trvale

10 Platnost a správa dokumentu

Vlastníkem tohoto dokumentu je Vedoucí oddělení IT, který musí nejméně jednou ročně dokument zkontrolovat a případně aktualizovat.

11 Příloha A – Seznam zpracovatelů

Amazon Web Services, Inc.

EMEA s.r.o.

ESA s.r.o.

Freshdesk Inc.

General Logistics Systems Czech Republic s.r.o.

Google Ireland Limited

Gransy s.r.o.

IPEX a.s.

Jaspar s.r.o.

One Click Business Solutions s.r.o.

PragueBest s.r.o.

SuperNetwork s.r.o.