**Vzor - Záznamy o činnostech zpracování**

| **#** | **Kategorie a charakteristiky zpracování osobních údajů** | **Komentáře pro vyplnění** |
| --- | --- | --- |
|  | Jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů [článek 30 odst. 1 písm. a) GDPR]: | Jméno a kontaktní údaje správce:  IEM Allergy s.r.o.  Padovská 696/3  109 00 Praha 10  Jiří Munk  Tel.: +420 602 134 1  e-mail: iemallergy@gmail.com  www.pkumaestro.cz |
|  | Identifikace příslušných zpracování osobních údajů [článek 30 odst. 1 písm. b) GDPR]: | * + - * 1. zákaznická (klientská) agenda;         2. obchod a marketing, komunikace online;         3. zaměstnanecká agenda |
|  | Proč (za jakým účelem) a na základě jakého právního titulu se osobní údaje v rámci zpracovávání zpracovávají [článek 30 odst. 1 písm. b) GDPR]? | **Klienti:** Zákaznický program – dobrovolně poskytnuté osobní údaje – online a offline komunikace s pacienty (vzorky, dárky)  **Třetí osoby**: oprávněný zájem správce – plnění smlouvy  s klientem; plnění právních povinností vyplývajících  z předpisů upravujících výkon advokacie  **Zaměstnanci:** pracovní smlouva, DPP, DPČ – plnění  povinností vyplývajících ze smluv se zaměstnanci a ze  zákoníku práce a zákona o zaměstnanosti |
|  | Jaké osobní údaje jsou zpracovávány v rámci zpracování [článek 30 odst. 1 písm. c) GDPR]? | **Klienti:** Viz údaje uvedené v registračním formuláři + link registrační formulář (zákazník/zástupce)  Jméno zástupce osoby s PKU, Příjmení zástupce osoby s PKU, Jméno osoby s PKU, Příjmení osoby s PKU, Datum narození osoby s PKU (pro dárek k narozeninám), Adresa (pro zasílání dárků), Ulice a ČP, Město, PSČ, Stát, Telefon, E-mail (pro nové PKU recepty a slevy), Který z našich produktů používá osoba s PKU?, Člen věrnostního programu PKU Maestro, Metabolické centrum, Ošetřující lékař  **Třetí osoby**: jméno a příjmení, adresa do práce, telefon, e-mail  **Zaměstnanci:** jméno, adresa, datum narození, bankovní  účet, pracovní doba, rodinný stav, vzdělání, fotografie |
|  | Z jakých zdrojů jsou osobní údaje získány [článek 30 odst. 1 písm. c) GDPR]? | Zákazníci - Pacienti PKU, jejich zástupci  Lékárnice  Ošetřující lékaři |
|  | Kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích: | Viz seznam zpracovatelů  - Účetní (samostatná)  - IT firma udržující náš systém |
|  | V jakém termínu a jak se osobní údaje likvidují [článek 30 odst. 1 písm. f) GDPR]? | Viz bod 2 Ochrana osobních údajů |
|  | Jakým způsobem se osobní údaje aktualizují [článek 30 odst. 1 písm. g) GDPR]? | Informacemi od subjektů údajů - online v rámci registračního účtu, provádí přímo zákazník |
|  | Které listinné a elektronické evidence (archivy, IT systémy, datová úložiště) provádějí zpracování [článek 30 odst. 1 písm. g) GDPR]? | Pro vedení klientské agendy používáme systém  s názvem Anabix – CRM systém.  Přístup do tohoto systému je chráněn heslem unikátním  pro každého uživatele.  Drupal 8 |
|  | Je prostředí pravidelně bezpečnostně testováno (zejm. IT systémy)? Interně nebo externími konzultanty? [článek 30 odst. 1 písm. g) GDPR]. | Pravidelně se provádí funkcionální testování, o bezpečnost systému Drupal se stará jeho bezpečnostní tým, který pravidlně vydává aktualizace. |
|  | Jak je zajištěna bezpečnost předání dat při klientské komunikaci [článek 30 odst. 1 písm. g) GDPR]? | Web, kde se může klient registrovat, je dostupný pouze přes HTTPS. Dále se prostřednictvím API systému Anabix (je nutné se autorizovat) data synchronizují. |
|  | Jak je zajištěna bezpečnost sdílení dat s externími subjekty? Mají všichni externí dodavatelé, zpracovávající osobní údaje, uzavřené smlouvy o zpracování osobních údajů, poskytující odpovídající záruky ochrany [článek 30 odst. 1 písm. g) ve spojení s článkem 28 GDPR]? | Ano. Smlouvy o zpracování osobních údajů máme  uzavřeny s následujícími dodavateli:  - Účetní (společnost, samostatná)  - IT pracovník udržující náš systém  - více viz seznam zpracovatelů  CRM systém – chráněn unikátním heslem |
|  | Je zajištěna nevratná likvidace dat v rámci databázového systému [článek 30 odst. 1 písm. g) GDPR]? | Ano, data jsou likvidována, nejen deaktivována. Nevymazávají se zálohy. |
|  | Je k dispozici procedura k určení práv subjektů údajů a jejich výkon s ohledem na jejich data, která jsou zpracovávána v rámci zpracování? | Ano, umožňujeme každému podat žádost na našem webu,  žádosti vyřizujeme v předepsaných lhůtách. |
|  | Poskytují se oprávněným subjektům údajů předepsané informace, zejména o:   * rozsahu a účelu zpracování, * způsobu zpracování osobních dat, * komu mohou být osobní údaje zpřístupněny? | Ano, informace poskytujeme následující formou:  - na našem webu www.pkumaestro.cz  - ve smlouvě s klienty  - v odpovědích na žádosti subjektů údajů  Na webové stránce [www.pkumaestro.cz](http://www.pkumaestro.cz/) je souhlas, žádost subjektu údajů i seznam zpracovatelů. |
|  | Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému anebo neoprávněnému přístupu k osobním údajům, jejich změně, zcizení, zneužití, zničení nebo ztrátě [článek 30 odst. 1 písm. g) GDPR]? | Ano, uplatňujeme zejména následující opatření:  K zpracovávaným údajům mají přístup pouze  osoby, které s údaji pracují;  - Údaje jsou zaheslované v počítači v rámci systému Anabix; údaje v listinné podobě se nacházejí v uzavřených skříních;  - Přístup do kanceláří je zabezpečen bezpečnostním zámkem;  - IT systém je standardní, vyzkoušený. Přístup do IT  systému je omezen podle nastavených manažerských rolí.  - IT systém je pravidelně testován a udržován  externím dodavatelem, se kterým jsme uzavřeli  smlouvu o zpracování osobních údajů. |
|  | Jsou zpracovávané osobní údaje přenášeny do zahraničí nebo jsou přístupné ze zahraničí [článek 30 odst. 1 písm. e) GDPR]? | Pouze v rámci EU, mimo EU údaje neposkytujeme |
|  | Jsou pracovníci, mající přístup k osobním údajům v rámci zpracování osobních údajů, proškoleni? Mají tito pracovníci ve svých smlouvách sjednánu povinnost mlčenlivosti ve vztahu ke zpracovávaným osobním údajům [článek 30 odst. 1 písm. g) GDPR]? | Všichni zaměstnanci jsou proškoleni a zavázáni k mlčenlivosti, externí dodavatelé mají uzavřenou smlouvu o zpracování. |