ІНФОРМАЦІЯ ПРО ЗАХИСТ ТА АДМІНІСТРУВАННЯ ДАНИХ

Фірма PS Sol - PC Ker Kft.

Дата набрання чинності: з 1-го липня 2020 року

Фірма PS Sol - PC Ker Kft (головний офіс: Угорщина, 11063 Budapest, Szinyei Merse utca 10, реєстраційний номер підприємства: 03-09-126056, податковий номер: 24136231-2-42, представник: Міклош Сабадош, e-mail: pskerkft@gmail.com, номер телефону: +36 70 362 1047 (далі іменована як "компанія") надає інформацію про свою діяльність з адміністрування даних відповідно до Постанови Європарламенту та Європейської Ради № 2016/679 про загальне регулювання захисту даних (далі іменоване як GDPR).

1. Наша ділова активність з адміністрування даних:

Компанія виступає в якості адміністратора даних щодо персональних даних, що відносяться до наступних видів діяльності:
• прийом заявок від Клієнтів, пропозиції на послуги, що надаються, укладення контрактів,
• підтримка ділових відносин з клієнтами,
• створення та обслуговування зайнятості, підбір персоналу.

2. Обсяг персональних даних, якими управляє наша компанія:

У процесі адміністрування даних, компанія запитує у фізичних осіб наступні дані: ім'я, адреса, дівоче ім'я матері, місце і дату народження, номер посвідчення особи (паспорта), номер телефону, адреса електронної пошти (у співробітників компанії - номер соціального страхування, податковий номер, номер водійського посвідчення), або ім'я, номер телефону, Адреса електронної пошти контактної особи в разі не фізичних (юридичних) осіб.

3. Мета ділової активності Компанії при адмініструванні персональних даних:

Компанія обробляє персональні дані, якими вона управляє, для здійснення наступних цілей:
• для укладення та виконання договорів, необхідних для здійснення її економічної діяльності, для пред'явлення претензій і примусового виконання вимог, обов'язків і прав, які випливають з цих договорів, для контактів з клієнтами і для виставлення рахунків;
• для відправки регулярних інформаційних листів, пов'язаних зі спільним бізнесом;
• для вироблення ділової та маркетингової стратегії, для ведення інформаційних даних партнерів з метою проведення ділових заходів;
• ведення встановленого законом обліку співробітників, звітності, підготовка декларацій і заяв, дотримання прав і обов'язків, що випливають із законодавства з працевлаштування;
• набір і відбір потенційних співробітників;
• забезпечення дотримання законних інтересів адміністратора даних.

Компанія має право обробляти персональні дані, необхідні для досягнення будь-якої з описаних вище цілей адміністрування даних.
Компанія не буде використовувати надану персональну інформацію в цілях, які відрізняються від описаних в цих пунктах.

4. Правові основи діяльності компанії з адміністрування даних:

• Згода зацікавленої особи: добровільна згода користувача на адміністрування його персональних даних на основі отримання відповідних роз'яснень відповідно до вимог загальних Правил захисту даних (GDPR) стаття 6 абзац (1) пункт а);
• Виконання умов договору: Обробка даних необхідна для виконання зобов'язань такого договору, в якому зацікавлена особа є одним з учасників цього договору, відповідно до вимог загальних Правил захисту даних (GDPR) стаття 6 абзац (1) пункт б);
• Виконання юридичних зобов'язань: Обробка даних необхідна для виконання юридичних зобов'язань, обов'язкових для адміністратора цих даних (таких як ведення звітності, бухгалтерський облік,

дотримання зобов'язань за поданням даних в рамках трудового законодавства), відповідно до вимог загальних Правил захисту даних (GDPR) стаття 6 абзац (1) пункт в);
• Дотримання законних інтересів: Обробка даних необхідна для забезпечення законних інтересів адміністратора або третьої сторони, відповідно до вимог загальних Правил захисту даних (GDPR) стаття 6 абзац (1) пункт е).

5. Інформація про особу, яка обробляє інформацію:

Пані Ержебет Токодине (Tokodiné Erzsébet e.v.), в якості бухгалтера, проводить обробку даних, якими управляє компанія при виконанні обов'язків найму та нарахування заробітної плати співробітникам, а також Ержебет Токодине (Tokodiné Erzsébet e.v.), в якості бухгалтера, проводить обробку даних при виконанні завдань, пов'язаних з виставленням рахунків. Крім того фірма FEIGL AUDIT Kft, в якості аудитора, бере участь в адмініструванні даних як обробник цих даних. Фірма NETCLASS Kft є обробником даних в якості оператора інформаційної служби.

Трансляція даних обробнику інформації може здійснюватися без спеціальної згоди суб'єкта персональних даних. Розкриття персональних даних третім особам або органам влади може здійснюватися виключно на підставі вже прийнятого офіційного рішення, якщо інше не передбачено законом, або за умови попередньої явної згоди, отриманої від суб'єкта цих даних.

6. Пересилання даних:

Відповідно до вимог Закону, компанія зобов'язана пересилати в Національне податкове і митне управління Угорщини (NAV) всю інформацію і реквізити про Покупця, про продавця, про статті товарів і послуг або інших уточнюючих відомостях, зазначених у виставлених рахунках клієнтів.

Компанія не передає жодних даних третій державі, яка не є стороною регулювання відповідно до загальних правил захисту даних (GDPR). Така інформація надається виключно зазначеному в цьому роз'ясненні обробнику, і тільки лише для зазначених цілей застосування.

7. Принципи адміністрування даних в компанії (далі названий як "адміністратор даних"):

Адміністратор даних зобов'язаний підкорятися принципам сумлінності, цілісності та прозорості при обробці персональних даних, а також обробляти інформацію відповідно до положень чинного закону та цього роз'яснення.

Адміністратор даних може вимагати інформацію для виконання послуг, які він надає, виключно на підставі добровільної згоди відповідної особи, і ця інформація може бути використана тільки для цієї мети.

Адміністратор даних може обробляти дані тільки з метою, зазначених у цьому роз'ясненні та передбачених у відповідному законодавстві. Обсяг оброблюваних персональних даних пропорційний масштабу мети обробки даних і не повинен виходити за її межі.

Адміністратор інформації не має права обробляти персональну інформацію осіб, які не досягли віку 18 років.

Адміністратор даних не займається перевіркою наданих персональних даних. За адекватність наданих персональних даних несе відповідальність тільки та особа, яка їх надала.

Адміністратор даних не має права передавати персональну інформацію, що знаходиться в його розпорядженні та зібрану для цілей обробки інформації, зазначених у цьому роз'ясненні, ніякій третій стороні, за винятком деяких випадків дотримання конкретних зобов'язань перед державними організаціями при виконанні і вимог законодавства і цього припису.

У деяких випадках адміністратор даних може зробити доступною особисту інформацію порушеного суб'єкта для третіх осіб - у зв'язку з офіційним проханням від судових або поліцейських органів, в зв'язку з

юридичною процедурою в області авторського права, майна або іншого порушення або юридично обґрунтованої підозри у діях порушеного суб'єкта з метою порушення законних інтересів адміністратора даних з надання інформаційних послуг і т. д.

Адміністратор даних забезпечує безпеку обробки персональних даних, приймає технічні та організаційні заходи безпеки і встановлює правила процедури для забезпечення того, щоб зібрані, збережені або оброблювані дані були захищені з метою запобігти випадковим втратам, незаконне знищення, несанкціонований доступ, незаконне використання або несанкціоновані зміни даних і поширення. Для виконання цієї вимоги, адміністратор даних повинен вступати в контакт з будь-якою третьою стороною, якій він передає ці персональні дані.

З урахуванням відповідних положень загальних Правил захисту даних (GDPR) адміністратор даних не є зобов'язаним призначати співробітника, відповідального за захист інформації.

8. Доступ співробітників компанії до персональних даних:

Компанія має право надавати своїм співробітникам доступ тільки до тих персональних даних, якими вони безпосередньо керують, і для надання тільки тих послуг, які строго необхідні для здійснення цієї роботи. Весь доступ суворо реєструється, і тільки оператор інформаційної служби має доступ до функції вилучення і передачі даних.

Операції резервного копіювання даних виконуються адміністратором даних шляхом шифрування відповідної інформації за допомогою обробника даних, що дозволяє в разі необхідності відновлення відповідної інформації зробити так, що співробітники не матимуть доступу до збережених персональних даних. Співробітники компанії не мають доступу до серверів даних в реальному часі.

9. Права порушеного суб'єкта на звернення до його персональних даних:

9.1. Право доступу до інформації:

Суб'єкт персональних даних має право вимагати від компанії повідомити йому про той факт, що чи дійсно Компанія управляє персональними даними суб'єкта, і, якщо це так, то він може зажадати надати йому доступ до персональних даних, які компанія адмініструє. Суб'єкт даних може запросити інформацію про адміністрування його персональних даних у будь-який час, у письмовій формі, рекомендованим листом або листом з повідомленням, надісланим на адресу компанії, або електронною поштою: pskerkft@gmail.com з отриманням запитаної інформації на адресу своєї електронної пошти. Надісланий у листі запит про надання інформації вважається достовірним, якщо на підставі цього запиту можна чітко ідентифікувати зацікавлену особу. Відправлений по електронній пошті запит на інформацію вважається достовірним тільки в тому випадку, якщо він відправлений суб'єктом даних з такої ж адреси електронної пошти, який був заздалегідь наданий компанії, однак це не може перешкоджати компанії ідентифікувати суб'єкта персональних даних іншим способом, ще до моменту надання запитаної інформації.

Запит персональної інформації може включати відомості про суб'єкт даних, керованих компанією, їх джерело, мета використання, юридичне обґрунтування, тривалість, ім'я та адресу будь-якого іншого обробника даних, чия діяльність пов'язана з обробкою цих даних.

9.2. Право на виправлення:

Суб'єкт персональних даних має право вимагати виправлень, уточнень або зміни оброблюваних компанією персональних даних. Беручи до уваги мету обробки даних, суб'єкт даних може запросити додавання інформації в неповні персональні дані. Після того як був зроблений запит на зміну персональних даних, попередні (видалені) дані вже не можуть бути відновлені.

9.3. Право на видалення інформації:

Суб'єкт даних може вимагати видалення оброблюваних компанією персональних даних.

У видаленні інформації може бути відмовлено:
• внаслідок здійснення права на вільне вираження думок і поширення інформації; або
• якщо така обробка персональних даних обумовлена положеннями законів; і
• якщо така обробка необхідна для того, щоб подавати, приводити у виконання або захищати судові позови.

У будь-якому випадку компанія зобов'язана проінформувати суб'єкта персональних даних про відмову у видаленні відповідної інформації, вказавши причини відмови у видаленні. Після виконання запиту на видалення персональних даних попередні (видалені) дані не можуть бути відновлені.

9.4. Право на обмеження обробки даних:

Суб'єкт даних може вимагати, щоб адміністратор обмежив обробку його персональних даних у тому випадку, якщо суб'єкт даних оскаржує точність оброблюваних персональних даних. У цьому випадку обмеження поширюється на той період часу, протягом якого компанія матиме можливість перевірити точність персональних даних. Компанія повинна вказати персональні дані, якими вона керує, якщо суб'єкт даних оскаржує їх правильність або точність, але правильність або неточність оспорюваних персональних даних не може бути чітко встановлена. Зацікавлена сторона також може попросити, щоб обробка персональних даних адміністратором даних була б обмежена, якщо мета адміністрування даних реалізована, але зацікавлена сторона і далі вимагає адміністрування цих даних, для обробки юридичних претензій, які вже подані, здійснюються або захищаються.

9.5. Право на протест:

Суб'єкт даних може подати протест проти обробки його персональних даних:
• якщо обробка цих персональних даних проводиться виключно з метою виконання юридичних зобов'язань адміністратора даних, або необхідні для здійснення законних інтересів адміністратора або третьої особи;
• коли метою адміністрування даних є безпосереднє придбання прибутку, опитування громадської думки або наукові дослідження; або
• коли адміністрування даних здійснюється для задоволення завдань публічного інтересу.

Адміністратор даних перевіряє правове обґрунтування протесту від суб'єкта даних і, якщо встановлено, що протест має правове обґрунтування, адміністратор даних припиняє обробку цих персональних відомостей, і блокує подальшу обробку згаданих даних, повідомляє про це всіх осіб, яким раніше вже були передані персональні дані, на які поширюється цей протест.

9.6. Право відкликати вже подану згоду:

Суб'єкт даних у будь-який час має право відкликати свою згоду на обробку даних, оброблюваних до цього моменту за його згодою. Відкликання такої згоди не завдає шкоди законності обробки даних до моменту відкликання згоди. Відкликання своєї згоди Ви можете зробити по інтернету, пославши таке відкликання за адресою електронної пошти pskerkft@gmail.com.

9.7. Право на переносимість інформації:

Суб'єкт даних може вимагати, щоб ці персональні дані були надані йому на паперовому носії, або в структурованому, широко використовуваному електронному форматі (XML/XLS/CSV) і / або, за запитом суб'єкта даних, можуть бути передані цим адміністратором даних іншому адміністратору даних.

10. Безпека даних:

Для захисту інформаційних даних компанією були введені і застосовані наступні заходи інформаційної обережності та безпеки:

10.1. Фізична безпека

У головному офісі є електронна система санкціонованого доступу і служба контролю на вході. У головному офісі і в службових приміщеннях компанії є система камер спостереження, що забезпечує безпеку від несанкціонованого проникнення або силового вторгнення, пожежі або стихійного лиха. Оброблювані на паперовій основі дані зберігаються в ізольованому місці, доступ до якого можуть відкрити тільки ті, у кого є відповідні права доступу.

10.2. Безпека даних в інформаційній інфраструктурі

Персональні дані зберігаються на серверах, наданих хостинг-провайдером, доступ до яких може отримати тільки дуже обмежений службовий персонал або група співробітників відповідно до суворої політики конфіденційності. Системи інформаційної безпеки регулярно і багаторазово проходить повторне тестування і моніторинг для забезпечення та підтримки безпеки даних та інформаційних технологій. Офісні робочі станції захищені паролем, використання сторонніх носіїв інформації строго регулюється і допускається тільки на безпечних умовах після ретельної перевірки. Безперервно працює та забезпечується систематичний захист від шкідливого програмного забезпечення, що охоплює всі наші системи або окремі елементи системи. Проектування, розробка, тестування та експлуатація програм, додатків та інструментів повинні проводитися з пріоритетом функцій безпеки та ізоляцією таких процесів.

10.3. Безпека інформації в каналах зв'язку

Що стосується переданих електронними засобами повідомлень і файлів, з метою виконання необхідних вимог до безпечного обміну інформацією, ми забезпечуємо цілісність даних як для адміністрування (цілі забезпечення зв'язку), так і для користувача даних. Процедури виявлення і виправлення помилок використовуються з метою уникнення втрати та пошкодження переданих даних. Що стосується додатків, то паролі, привілеї та інших параметри або дані, що відносяться до інформаційної безпеки, можуть бути передані тільки в зашифрованому вигляді. Ми запобігаємо втраті та пошкодженню даних за допомогою процедур виявлення та корекції втрат і пошкоджень переданих даних, та дбаємо про те, щоб безвідмовність системи була б повністю забезпечена. У випадку мережі, що використовується для трансляції даних, ми забезпечуємо запобігання незаконне з'єднання та перехоплення інформації всіма способами відповідними рівню безпеки.

10.4. Безпека даних при адмініструванні файлів

Крім того, ми також дотримуємося вимог безпеки даних, які викладені в правилах адміністрування записів і файлів. Адміністрування файлами повинно здійснюватися відповідно до рівнів прийнятності, як визначено в письмовому вигляді, відповідно до стандартів безпеки, застосовуваними до конфіденційності кожного документа. У нас є докладні та суворі правила знищення, зберігання, або публікації документів.

11. Заходи, що застосовуються у разі виникнення інцидентів із захистом даних

Будь-які інциденти у зв'язку із захистом даних, які можуть виникнути, будуть повідомлені наглядовому органу відповідно до приписів законодавства протягом 72 годин з моменту отримання інформації про виникнення інциденту із захистом даних, та ми також ведемо облік всіх подібних інцидентів. У передбачених законом випадках, суб'єкти даних також отримують інформацію про такі інциденти.

12. Тривалість адміністрування даних

Інформація та дані, що містяться в укладеному з клієнтом договорі, зберігаються протягом п'яти років після виконання договору.

З метою дотримання вимог бухгалтерського та податкового законодавства, персональні дані зберігаються протягом семи років після закінчення податкового року.

Виписки з трудових книжок про зайнятість і трудові відносини зберігаються протягом 4 років після припинення трудових відносин.

Персональні дані, надані при підписці на розсилку, зберігаються 3 роки.

13. Варіанти для забезпечення дотримання законності

Ви можете зв'язатися з компанією з будь-яких питань або зауважень у зв'язку з адмініструванням даних:
по електронній пошті: pskerkft@gmail.com
за номером телефону: +36 70 362 1047

Скарга суб'єкта даних щодо адміністрування даних, може бути подана безпосередньо в Національне управління із захисту даних та свободи інформації (адреса: Угорщина, 1125 Budapest, Szilágyi Erzsébet fasor 22/C;
телефон: + 36-1-391-1400;
електронна пошта: ugyfelszolgalat@naih.hu;
веб-сайт: www.naih.hu).

У разі порушення законних прав суб'єкта даних, можна звертатися до суду. Суд має юрисдикцію для розгляду та прийняття рішення за позовом. За вибором суб'єкта даних, позов може бути поданий до суду або за місцем проживання суб'єкта, або за місцем проживання відповідної особи. За запитом адміністратор інформує користувача про можливості та засоби відшкодування збитку.

14. Терміни, що використовуються в цьому інформаційному документі:

14.1. "***Персональні дані***" - означають будь-яку інформацію, що відноситься до вже ідентифікованого фізичній особі або до особи, яка слід ідентифікувати (надалі тексті - "суб'єкт даних"); фізична особа може бути ідентифікована, якщо вона прямо або побічно може бути ідентифікована за деякими критеріями, зокрема, за допомогою спеціального ідентифікатора, такого як ім'я, номер, дані про місцезнаходження, онлайн-ідентифікатор, або один або кілька факторів, які відносяться до фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї фізичної особи;

14.2. "***Адміністрування даних***" означає будь-яку операцію або набір операцій, що виконуються з персональними даними або файлами, будь то автоматизовані або неавтоматизовані операції, такі як збір, реєстрація, організація, компонування, зберігання, перетворення або зміна, опитування, запит, використання, розкриття шляхом трансляції, поширення або іншого надання інформації, узгодження або з'єднання подібних даних, обмеження, видалення або знищення;

14.3. "***Адміністратор даних***" означає будь-яку фізичну або юридичну особу, орган державної влади, агентство чи будь-який інший орган, який визначає цілі і засоби обробки персональних даних, індивідуально або спільно з іншими особами; якщо цілі і засоби обробки визначаються законодавством Союзу держав або національним законодавством, адміністратор або конкретні критерії для призначення адміністратора даних також можуть визначатися законодавством Союзу держав або національним законодавством;

14.4. "***Обробник даних***" означає будь-яку фізичну або юридичну особу, орган державної влади, агентство або будь-який інший орган, який обробляє персональні дані від імені адміністратора даних;

14.5. "***Згода суб'єкта даних***" означає добровільне, конкретне і однозначне вираження волевиливу суб'єкта даних, яке зрозуміло грунтується на відповідному інструктажі, за допомогою якого суб'єкт даних заявляє, або недвозначно діє в якості підтвердження його волевиливу, що він погоджується на обробку його персональних даних;

14.6. "***Інцидент із захистом даних***" означає шкоду безпеці, спричинену випадковим або незаконним знищенням, втратою, зміною, несанкціонованим розкриттям або доступом до персональних даних, що транслюються, зберігаються або іншим чином обробляються.

г. Будапешт, 1-го липня 2020 року

PS Sol - PC Ker Kft.