Політика компанії "АРЕНСІЯ" [ARENSIA] у сферах конфіденційності та захисту даних

I. Політика захисту даних

В рамках своєї діяльності компанія "АРЕНСІЯ Експлораторі Медісін" [ARENSIA Exploratory Medicine] забезпечує необхідну відповідність високому рівню захисту персональних даних та вимогам багатогранних положень Загального регламенту ЄС про захист даних (GDPR). Ця політика стосується всіх сторін - працівників, постачальників, пацієнтів та спонсорів - які надають нашій компанії будь-які обсяги інформації.

Ця Політика захисту даних застосовується до компанії "АРЕНСІЯ Експлораторі Медісін" [ARENSIA Exploratory Medicine] в усіх країнах світу та ґрунтується на всесвітньо визнаних фундаментальних принципах захисту даних. Для цілей транскордонної передачі даних між підрозділами компаній ця політика містить одну з необхідних рамкових умов, що забезпечує належний рівень захисту даних, передбачений Загальним регламентом ЄС про захист даних[1].

II. Застосування національного законодавства

Загальний регламент ЄС про захист даних застосовується не тільки до організацій, розташованих у межах ЄС, але і до організацій, розташованих за межами ЄС, якщо вони пропонують товари чи послуги суб'єктам даних ЄС або здійснюють моніторинг їхньої поведінки. Він застосовується до всіх компаній - резидентів Європейського Союзу, які обробляють та утримують персональні дані суб'єктів даних, незалежно від місцезнаходження компанії.

III. Політика захисту даних - Визначення термінів

"Персональні дані" означає будь-яку інформацію, що стосується фізичної особи, що була ідентифікована чи може бути ідентифікована; фізична особа ("суб'єкт даних"), що може бути ідентифікована - це особа, що може бути ідентифікована, прямо чи непрямо, зокрема, на основі будь-якого ідентифікатора, такого як прізвище, ідентифікаційний номер, дані про місцезнаходження, Інтернет-ідентифікатор, чи на основі одного чи кількох факторів, притаманних фізичній, фізіологічній, генетичній, ментальній, культурній чи соціальній приналежності такої фізичної особи;

"Обробка" означає будь-яку операцію або сукупність операцій, таких як збирання, реєстрація, організація, структурування, зберігання, адаптування, зміна, отримання, консультація, використання, розкриття шляхом передачі, поширення чи надання іншим чином, вивірення або об'єднання, обмеження, видалення або знищення персональних даних чи груп персональних даних, у тому числі з використанням автоматизованих систем.

"*Контролер*" означає фізичну або юридичну особу, державний орган, агентство або інший орган, який самостійно або спільно з іншими сторонами визначає цілі та засоби обробки персональних даних; якщо цілі та засоби такої обробки визначаються законодавством Союзу або Держави-члена, законодавством Європейського Союзу або Держави-члена може бути призначений контролер або визначені конкретні критерії для його призначення;

"Обробник" означає фізичну або юридичну особу, державний орган, агентство або інший орган, який обробляє персональні дані від імені контролера;

---

[1] Регламент (ЄС) 2016/679 (Загальний регламент ЄС про захист даних) - 2 редакція, 18 травня 2018 р.

"*Одержувач*" означає фізичну або юридичну особу, державний орган, агентство або інший орган, якому розкриваються персональні дані, незалежно від того, є чи не є він третьою стороною. Однак органи державної влади, які можуть отримувати персональні дані в рамках конкретного розслідування відповідно до законодавства Союзу або держав-членів, не вважаються одержувачами; обробка цих даних цими державними органами повинна відповідати чинним правилам захисту даних відповідно до цілей обробки;

"Третя сторона" означає фізичну або юридичну особу, державний орган, установу або орган, окрім суб'єкта даних, контролера, обробника та осіб, які, згідно з повноваженнями, наданими безпосередньо контролером або обробником, мають право обробляти персональні дані;

"Згода" суб'єкта даних означає будь-яке добровільно надане, конкретне, поінформоване та однозначне повідомлення про бажання суб'єкта даних, за допомогою якого він або вона заявою чи однозначною позитивною дією висловлює згоду на обробку персональної інформації, що стосується його або її;

"Транскордонна обробка" - обробка персональних даних, яка відбувається в контексті діяльності однієї установи контролера або обробника в Союзі, але яка істотно впливає або може істотно впливати на суб'єктів даних у більш ніж одній Державі-члені.

"Посадова особа з питань захисту даних" - особа, призначена контролером та обробником персональних даних для виконання завдань та обов'язків, визначених Союзом. Він/вона не отримує жодних вказівок щодо виконання ним/нею завдань, не може бути покараний за виконання своїх завдань, підпорядковується безпосередньо вищому керівництву і зобов’язаний зберігати таємницю або конфіденційність щодо виконання своїх завдань. Завдання Посадової особи з питань захисту даних визначені у розділі XII.

IV. Принципи обробки персональних даних

1. Законність, чесність і прозорість

Персональні дані повинні оброблятися законно, справедливо та прозоро по відношенню до суб’єкта даних.

2. Обмеження цілей

Персональні дані повинні збиратися для конкретних, явних та законних цілей і не оброблятися в подальшому способом, несумісним із цими цілями; подальша обробка для цілей архівування в суспільних інтересах, для цілей наукових чи історичних досліджень або статистичних цілей, відповідно до Статті 89(1)[2], не вважається несумісною з початковими цілями.

3. Мінімізація даних та точність

Зібрані персональні дані повинні бути адекватними, суттєвими та обмеженими тим, що необхідно для досягнення цілей, для яких вони обробляються. Дані повинні бути точними і, за необхідності, актуалізованими; необхідно вжити всіх розумних кроків для того, щоб персональні дані, які є неточними, з огляду на цілі, для яких вони обробляються, були негайно видалені або виправлені.

[2] Ст. 89 Загального регламенту ЄС про захист даних "Запобіжні засоби та обмеження, що стосуються обробки для цілей архівування в суспільних інтересах та для цілей наукових чи історичних досліджень"

4. Обмеження на зберігання

Персональні дані повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілей, для яких обробляються персональні дані; персональні дані можуть зберігатися протягом більш тривалих періодів, якщо персональні дані будуть оброблятися виключно для архівування в інтересах суспільства, для цілей наукових чи історичних досліджень або статистичних цілей відповідно до Статті 89(1)[3] за умови застосування відповідних технічних та організаційних заходів, що вимагаються цим Регламентом для забезпечення захисту прав та свобод суб'єкта даних.

5. Цілісність та конфіденційність

Зібрані дані повинні оброблятися таким чином, щоб забезпечити належний рівень безпеки персональних даних, включаючи захист від несанкціонованої чи незаконної обробки та випадкової втрати, знищення або пошкодження, з використанням відповідних технічних чи організаційних заходів.

V. Надійність обробки даних

Збір, обробка та використання персональних даних дозволяються лише з урахуванням викладених нижче правових основ Загального регламенту ЄС про захист даних. Конфіденційність та безпека зібраних персональних даних є пріоритетом для "АРЕНСІЯ Експлораторі Медісін" [ARENSIA Exploratory Medicine], і для компанії "АРЕНСІЯ" не менш важливим є забезпечення розуміння усіма того, як ми обробляємо ці дані:

1. Дані пацієнтів

Для проведення клінічного випробування відповідно до положень Гельсінської декларації та Міжнародного комітету з гармонізації (ICH) щодо Належної клінічної практики (GCP) ми збираємо дані в обсязі, описаному у схваленому та затвердженому голосуванням протоколі випробувань. Такі дані можуть включати інформацію, що стосується стану здоров'я, та іншу конфіденційну інформацію.

2. Дані співробітників

Для ведення бізнесу в глобальному масштабі та виконання вимог державних нормативних актів (про працевлаштування, оподаткування, страхування тощо) ми збираємо різні персональні та інші дані залежно від ваших трудових обов'язків, громадянства, місця роботи та інших факторів.

Такі дані можуть включати:

- Ім'я, прізвище;
- Ідентифікаційний номер;
- Номер телефону;
- Адресу ел. пошти;
- Банківські та інші фінансові дані;
- Державні ідентифікаційні номери, в т.ч. номери соціального страхування, ідентифікаційні дані платника податків, номер посвідчення водія;
- Дані про сім'ю.

[3] Ст. 89 Загального регламенту ЄС про захист даних "Запобіжні засоби та обмеження, що стосуються обробки для цілей архівування в суспільних інтересах та для цілей наукових чи історичних досліджень"

Ми можемо використовувати дані таким чином:

- для ідентифікації певної особи;
- для цілей обміну даними з будь-ким;
- для задоволення потреб у людських ресурсах;
- для виконання урядових приписів та постанов;
- для здійснення виплат працівникам (компенсації, медичне страхування, відшкодування витрат тощо).

3. Дані клієнтів та третіх сторін

Для ведення бізнесу та виконання договірних зобов'язань ми збираємо дані партнерів за договорами, таких як спонсори, субпідрядники та постачальники. Такі дані можуть включати назву, адресу електронної пошти компанії, номер телефону компанії, банківські та інші фінансові реквізити та дані компанії. Компанія "АРЕНСІЯ" вживає запобіжні заходи з метою забезпечити надання третім сторонам лише персональних даних, визначених інструкціями, та обмежити таке надання розкриттями даних агентам та субпідрядникам постачальника за умови отримання компанією "АРЕНСІЯ" попередньої письмової згоди від клієнта або третьої сторони, або забезпечити надання даних у випадках, коли відповідне розкриття інформації вимагається законом.

VI. Обробка даних контрактів

Обробка даних від імені когось означає, що провайдер залучається для обробки персональних даних, але не несе при цьому відповідальності за відповідний бізнес-процес. У цих випадках із зовнішніми провайдерами та афілійованими компаніями у складі "АРЕНСІЯ" повинна бути укладена Угода про захист даних від імені. Клієнт несе повну відповідальність за правильне виконання обробки даних. Провайдер може обробляти персональні дані лише згідно з інструкціями клієнта. Такі послуги можуть використовуватися для цілей обліку заробітної плати на місцях.

VII. Права суб'єкта даних

1. Право доступу

Частиною розширених прав суб'єктів даних, зазначених у Загальному регламенті ЄС про захист даних, є право суб'єктів даних отримувати від контролера даних підтвердження того, чи обробляються їхні персональні дані, де і з якою метою вони обробляються. Крім того, контролер зобов'язаний безкоштовно надати копію персональних даних в електронному форматі. Ця зміна є різким переходом до забезпечення прозорості даних та розширення можливостей суб'єктів даних.

2. Право на виправлення

Суб'єкт даних має право без зайвої затримки отримати від контролера виправлення неточних персональних даних, що стосуються його або її. Беручи до уваги цілі обробки, суб'єкт даних має право вимагати доповнення неповних персональних даних, у тому числі шляхом подання додаткової заяви.

3. Право на забуття

Відоме також як Стирання даних, право на забуття дає право суб'єкту даних вимагати від контролера даних видалення його/її персональних даних, припинення подальшого розповсюдження даних та потенційного припинення обробки даних третіми сторонами. Умови видалення включають дані, що більше не є

суттєвими для визначальних цілей обробки, або відкликання згоди суб’єктами даних. Слід також зазначити, що це право вимагає від контролерів порівнювати права суб'єктів із "суспільним інтересом у наявності даних" в процесі розгляді таких запитів.

4. Право на обмеження обробки

Умови отримання згоди посилюються, оскільки запит на згоду подається у зрозумілій та легкодоступній формі, при цьому до згоди додається інформація про мету обробки даних. Згода є чіткою та відмінною від інших питань та надається у зрозумілій та легкодоступній формі, використовуючи чітку та зрозумілу мову у кожному документі, наданому компанією "АРЕНСІЯ": трудові договори, договори з клієнтами та постачальниками, включаючи документи, надані Спонсорами через компанію "АРЕНСІЯ", тобто Форму надання інформованої згоди. Відкликати згоду так само легко, як і надати її.

5. Право на перенесення даних

Загальний регламент ЄС про захист даних створює можливість перенесення даних - право суб'єктів даних отримувати персональні дані щодо них, які вони раніше надавали у "загальноприйнятому та придатному для машинного зчитування форматі" і мають право передавати ці дані іншому контролеру.

6. Право на заперечення

Суб'єкт даних має право в будь-який час подати заперечення на підставах, що стосуються його чи її конкретної ситуації, проти обробки персональних даних, що стосуються його чи її, згідно з цими положеннями. Контролер втрачає право обробляти персональні дані, якщо контролер не продемонструє переконливі законні підстави для обробки, які переважають інтереси, права та свободи суб'єкта даних, або для встановлення, здійснення чи захисту законних вимог.

VIII. Конфіденційність обробки

На персональні дані поширюються вимоги щодо таємниці даних. Будь-який несанкціонований збір, обробка або використання таких даних працівниками заборонені. Будь-яка обробка даних, здійснена працівником, на яку він/вона не був уповноважений у рамках своїх законних обов'язків, є несанкціонованою. При цьому застосовується принцип службової необхідності. Працівники можуть мати доступ до персональної інформації лише у випадку, коли такий доступ узгоджується з типом відповідного завдання. Це вимагає ретельного розподілу, розмежування, а також реалізації ролей та обов'язків.

Співробітникам заборонено використовувати персональні дані для приватних або комерційних цілей, розкривати їх стороннім особам або надавати їх будь-яким іншим способом. Наглядові органи зобов'язані повідомляти своїх працівників на початку трудових відносин про обов'язок зберігати таємницю даних. Цей обов'язок залишається в силі навіть після закінчення трудової діяльності.

IX. Безпека обробки

Персональні дані повинні бути захищені від несанкціонованого доступу та незаконної обробки чи розкриття, а також від випадкової втрати, зміни або знищення. Це положення застосовується незалежно від того, в якому - електронному або паперовому - вигляді здійснюється обробка даних. До впровадження нових методів обробки даних, зокрема, нових IT-систем, необхідно визначити та реалізувати технічні та організаційні заходи щодо захисту

персональних даних. Ці заходи повинні здійснюватися із застосуванням найсучасніших засобів та з урахуванням ризиків обробки та необхідності захисту даних.

Зокрема, відповідальний відділ може проконсультуватися з представником департаменту IT та Посадовою особою з питань захисту даних. Технічні та організаційні заходи щодо захисту персональних даних є частиною обов'язків Посадової особи з питань захисту даних і повинні постійно коригуватися на основі технічних досягнень та з урахуванням організаційних змін.

X. Контроль захисту даних;

Відповідність Політиці захисту даних та чинному законодавству про захист даних регулярно перевіряється шляхом проведення аудиторських перевірок з питань захисту даних та застосування інших засобів контролю. Використання цих засобів контролю входить до обов'язків Посадової особи з питань захисту та інших підрозділів компанії, що мають права на аудит, або залучених зовнішніх аудиторів. Про результати контролю захисту даних необхідно повідомляти Посадову особу з питань захисту даних. Управлінський персонал компанії "АРЕНСІЯ Експлораторі Медісін" [ARENSIA Exploratory Medicine] має бути проінформований про основні результати шляхом отримання відповідної звітності. За запитом, результати контролю захисту даних будуть надані органу, відповідальному за захист даних. Відповідальний орган з питань захисту даних може здійснювати власний контроль за дотриманням положень цієї Політики в обсязі, дозволеному національним законодавством.

XI. Порушення безпеки даних, відповідальність та санкції

Запропоновані положення про витоки даних, насамперед, стосуються порушень положень корпоративної політики обміну повідомленнями. Інформація про витоки даних, що призводять до виникнення ризику для фізичних осіб (наприклад, несанкціоноване розкриття номера банківського рахунку або інформації про медичне страхування), має надаватися відповідному Агентству з питань захисту даних протягом 72 годин та постраждалим особам без зайвої затримки.

XII. Посадова особа з питань захисту даних

Посадова особа з питань захисту даних виконує роль лідера у сфері безпеки підприємства, як передбачено Загальним регламентом ЄС про захист даних. Посадові особи з питань захисту даних несуть відповідальність за нагляд за стратегією захисту даних та її реалізацією для забезпечення відповідності вимогам Загального регламенту ЄС про захист даних.

Обов'язки Посадової особи з питань захисту:

- Навчання компанії та співробітників важливим вимогам щодо відповідності законодавству
- Навчання персоналу, залученого до обробки даних
- Проведення аудитів для забезпечення відповідності та упереджувального вирішення потенційних проблем
- Виконання функцій ланки зв’язку між компанією та Наглядовими органами, створеними згідно з положеннями Загального регламенту ЄС про захист даних
- Моніторинг ефективності та надання інформації про результати діяльності у сфері забезпечення захисту даних

- Ведення комплексного обліку всіх заходів з обробки даних, що проводяться компанією, включаючи дані про цілі всіх видів обробки даних, які повинні бути оприлюднені за запитом

- Взаємодія з суб'єктами даних з метою проінформувати їх про те, як використовуються їхні дані, про їх права на видалення їх персональних даних та про те, які заходи компанія вжила для захисту їх персональної інформації.

XIII. Захист даних у компанії "АРЕНСІЯ"

Принципи, описані в цій політиці та передбачені вимогами Загального регламенту ЄС про захист даних, реалізуються в системах компанії "АРЕНСІЯ" шляхом затвердження відповідних Робочих інструкцій, що охоплюють згадані теми.