ЗАТВЕРДЖЕНО
Рішенням Наглядової Ради
Протокол засідання Наглядової Ради
ПрАТ «СК «Перша»
№58/2023 від 04.07.2023 р.
Голова Наглядової ради
_____ Сергій ВАСИЛИНА

ПОЛІТИКА
захисту персональних даних Приватного акціонерного товариства «Страхова компанія «Перша»

Київ, 2023 рік

ЗМІСТ

1. ВСТУП

1.1. Політика захисту персональних даних Приватного акціонерного товариства «Страхова компанія «Перша» (надалі – Політика) є внутрішнім документом Приватного акціонерного товариства «Страхова компанія «Перша» (надалі – Компанія), метою якого є встановлення адекватного рівня захисту даних, який має бути забезпечений в Компанії.
1.2. Ця Політика направлена на встановлення відповідних стандартів та вимог, які є обов'язковими для всіх працівників Компанії з метою побудови захисту персональних даних та виконання всіх вимоги, встановлених діючим законодавством.
1.3. Політика визначає цілі, завдання та принципи захисту персональних даних в Компанії та направлена на попередження та врегулювання ризиків, пов'язаних з обробкою, зберіганням та передачею персональних даних.
1.4. Політика затверджується Наглядовою радою Компанії та є обов'язковою до виконання всіма працівниками Компанії.
1.5. Політика переглядається щонайменше один раз на рік та доповнюється, якщо цього вимагають зміни в законодавчому чи організаційному середовищі Компанії.

2. ЗАГАЛЬНІ ПОЛОЖЕННЯ

2.1. Законодавство про захист персональних даних
Законодавчо захист персональних даних врегульовано Конституцією України, Законом України «Про захист персональних даних» (далі - Закон), іншими законами та підзаконними нормативно-правовими актами, міжнародними договорами України.
Захист персональних даних (особистих даних) є основним правом відповідно до ст. 7 Європейської конвенції про права людини та ст. 7 та 8 Хартії основних прав Європейського Союзу.
2.2. Термінологія
Володілець персональних даних - фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.
Згода суб'єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-комунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки.
Обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, оновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.
Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Розпорядник персональних даних - фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.
Суб'єкт персональних даних - фізична особа, персональні дані якої обробляються.

Інші терміни вживаються у значеннях, наведених в ст.2 Закону України «Про захист персональних даних» та/або в іноземних законодавчих актах.

2.3. Принципи обробки персональних даних

2.3.1. **Законність, справедливість та прозорість**: Персональні дані обробляються законно, справедливо та прозоро стосовно Суб'єкта даних.

2.3.2. **Призначення - обмеження**: Персональні дані збираються для визначених, явних та законних цілей і не піддаються подальшій обробці, яка не відповідає зазначеним цілям.

2.3.3. **Мінімізація даних**: Персональні дані повинні бути адекватними, релевантними та обмежуватись необхідними стосовно цілей, для яких вони обробляються.

2.3.4. **Точність**: Персональні дані повинні бути точними та, за необхідності, оновлюватися; необхідно зробити кожен розумний крок, щоб гарантувати, що неточності в персональних даних, беручи до уваги цілі, для яких вони обробляються, будуть негайно стиратися чи виправлятися.

2.3.5. **Обмеження зберігання**: Персональні дані зберігаються у формі, яка дозволяє ідентифікувати Суб'єктів даних не довше, ніж це необхідно для цілей, для яких вони обробляються.

2.3.6. **Цілісність та конфіденційність**: Персональні дані обробляються таким чином, що забезпечує належну безпеку Персональних даних, включаючи захист від несанкціонованої чи незаконної обробки та від випадкової втрати, знищення чи пошкодження, використовуючи відповідні технічні чи організаційні заходи.

2.4. Види персональних даних

2.4.1. **Загальні персональні дані:** будь-яка інформація, що стосується ідентифікованої фізичної особи, наприклад ім'я, ідентифікаційний номер, електронна адреса, дата народження.

2.4.2. **Спеціальні категорії персональних даних:** расове чи етнічне походження, політичні думки, релігійні чи філософські переконання чи членство в профспілках та обробка генетичних даних, біометричних даних з метою однозначної ідентифікації фізичної особи, даних, що стосуються стану здоров'я чи даних що стосується статевого життя фізичної особи чи сексуальної орієнтації

2.4.3. **Персональні дані, що стосуються кримінальних судимостей та правопорушень:** кримінальних судимостей та правопорушень або пов'язаних із ними заходів безпеки.

2.4.4. Відмінність видів персональних даних особливо важлива через наслідки, які може мати для Суб'єкта даних незаконна обробка. Наприклад, незаконне розголошення повних медичних звітів, включаючи хвороби, операції чи генетичні стани, може бути більш серйозним для Суб'єкта даних, ніж незаконне розголошення адреси електронної пошти після хакерської атаки.

2.5. Підстави для обробки персональних даних

Компанія може обробляти персональні дані виключно на таких підставах:

- згода суб'єкта персональних даних на обробку його персональних даних;
- дозвіл на обробку персональних даних, наданий Компанії як володільцю персональних даних відповідно до Закону виключно для здійснення його повноважень;
- укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
- захист життєво важливих інтересів суб'єкта персональних даних;
- необхідність виконання обов'язку Компанією як володільця персональних даних, який передбачений законом;
- необхідність захисту законних інтересів Компанії як володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту

основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

ВАЖЛИВО!

Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних, **за виключенням, якщо така обробка здійснюється на підставі однієї з наступних умов:**

- здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;
- необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до Закону із забезпеченням відповідного захисту;
- необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;
- здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до Закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;
- необхідна для обґрунтування, задоволення або захисту правової вимоги;
- необхідна в цілях охорони здоров'я для:
  - встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг тощо;
  - контролю якості надання медичних послуг за умови, що такі дані обробляються працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері контролю якості надання медичних послуг;
  - обміну інформацією про фінансування медичних послуг та послуг у сфері охорони здоров'я за умови, що такі дані обробляються працівниками Фонду соціального страхування України, Пенсійного фонду України, Фонду соціального захисту осіб з інвалідністю, центрального органу виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, на яких покладено обов'язки щодо забезпечення захисту персональних даних.
  - цілей забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів (в обсягах даних, зазначених у статті 7 Закону України "Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів");
  - вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;
  - даних, які були явно оприлюднені суб'єктом персональних даних.

3. ОРГАНІЗАЦІЯ ПРОЦЕСІВ

3.1. Особа, відповідальна за захист даних

3.1.1. В Компанії відповідальною особою за захист персональних даних є Головний комплаєнс-менеджер, до основних завдань якого відносяться:

- Консультувати працівників Компанії у питаннях захисту даних.
- Контролювати відповідність процедур Компанії вимогам чинного законодавства щодо захисту персональних даних та цієї Політики.
- Підвищення рівня обізнаності та навчання персоналу, що бере участь у операціях з обробки персональних даних.
- Проведення аудиту дотримання вимог чинного законодавствам щодо захисту персональних даних та цієї Політики.
- Представництво інтересів Компанії в комунакаціях з відповідними державними органами з питань захисту персональних даних.
- Проведення консультації, коли це необхідно, стосовно будь-яких питань, пов'язаних із захистом персоналльних даних.

3.1.2. Особа, відповідальна за захист персональних даних, звітує безпосередньо Наглядовій раді Компанії.

3.2. Дотримання прав суб'єкта персональних даних

Компанія забезпечує дотримання прав суб'єктів персональних даних, до яких, зокрема, відносяться такі права як:

- знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;
- доступ до своїх персональних даних;
- отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;
- пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- звертатися із скаргами на обробку своїх персональних даних до уповноваженої особи Компанії або до суду;
- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
- вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
- відкликати згоду на обробку персональних даних;
- знати механізм автоматичної обробки персональних даних;
- на захист від автоматизованого рішення, яке має для нього правові наслідки.

3.3. Повідомлення про порушення даних

Порушення даних означає порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розголошення або доступу до персональних даних, що передаються, зберігаються або обробляються іншим чином.

Несанкціонована або незаконна обробка може включати розкриття персональних даних або доступ одержувачами, які не мають права отримувати або мати доступ до даних, або будь-яка інша форма обробки, яка порушує вимоги чинного законодавства.

Наслідком порушення даних є те, що Володілець або Розпорядник персональних даних не в змозі забезпечити дотримання принципів, пов'язаних з обробкою персональних даних, визначених у чинному законодавстві.

Особа, відповідальна за захист персональних даних у Компанії, повинна бути інформована про будь-яке порушення даних. Таке повідомлення має бути здійснене негайно особою, яка таке порушення виявила.

Будь-які порушення даних повинні бути задокументовані, включаючи вжиті заходи для уникнення негативних наслідків для суб'єктів даних та майбутніх порушень даних.

3.4. Зберігання даних

Дотримання принципу обмеження зберігання, а також принципу точності здійснюється в Компанії у відповідності до внутрішніх нормативних документів щодо інформаційної безпеки та захисту інформації. Персональні дані, які більше не потрібні для цілей, для яких вони були зібрані та оброблені, повинні бути видалені або анонімізовані. Для встановлення відповідного терміну збереження повинні враховуватися норми чинного законодавство та/або законні інтереси Володільця персональних даних.

3.5. Передача даних

Передача даних означає будь-яку передачу персональних даних іншому Володільцю чи Розпоряднику або будь-якій третій стороні. Вимоги до передачі персональних даних, передбачені чинним законодавством та/або цією Політикою, повинні бути враховані у договірних положеннях щодо передачі персональних даних.

3.6. Навчання працівників

Особа, відповідальна за захист персональних даних, повинна проводити базове навчання щодо поводження з персональними даними для всіх працівників, які регулярно працюють з персональними даними.

Інколи може бути необхідне спеціальне навчання для всіх або певної групи працівників, наприклад, після порушення даних або змін в нормах чинного законодавства.

Кожен навчальний захід повинен бути документально підтверджений.

3.7. Звітність

Особа, відповідальна за захист персональних даних, регулярно звітує Наглядовій раді не рідше ніж 1 раз на рік.

Цей звіт включає щонайменше наступні пункти:

- Результати перевірок / візитів з боку наглядових органів з питань захисту даних та впровадження заходів, якщо такі є.
- Повідомлення від суб'єктів даних, адресовані Компанії щодо їхніх персональних даних, та результати їх розгляду.
- Результати проведених навчальних заходів.