Додаток №3 до наказу № 03-ПДн від 01 грудня 2019

ПОЛОЖЕННЯ
ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

м. Київ, 2019 р.

ЗМІСТ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Положення про обробку персональних даних у ТОВ "СПА ФІНАНС «(далі – Положення) розроблено відповідно до законодавства України, Трудового кодексу України (далі – ТК України), а також» переліком відомостей конфіденційного характеру", затвердженим Указом Президента України від 06.03.1997 № 188.

Це Положення визначає порядок обробки персональних даних і встановлює загальні вимоги до забезпечення безпеки персональних даних, що обробляються в ТОВ «СПА ФІНАНС» (далі – Оператор) як з використанням засобів автоматизації, так і без використання таких коштів.

У положенні використовуються такі основні поняття:

автоматизована обробка персональних даних-обробка персональних даних за допомогою засобів обчислювальної техніки;

блокування персональних даних-тимчасове припинення обробки персональних даних (за винятком випадків, якщо обробка необхідна для уточнення персональних даних);

інформаційна система персональних даних-сукупність містяться в базах даних персональних даних і забезпечують їх обробку інформаційних технологій і технічних засобів;

знеособлення персональних даних-дії, в результаті яких неможливо визначити без використання додаткової інформації приналежність персональних даних конкретному суб'єкту персональних даних;

обробка персональних даних - будь-яка дія (операція) або сукупність дій (операцій), що здійснюються з використанням засобів автоматизації або без використання таких засобів з персональними даними, включаючи збір, запис, систематизацію, накопичення, зберігання, уточнення (оновлення, зміна), Витяг, використання, передачу (поширення, надання, доступ), знеособлення, блокування, видалення, знищення персональних даних;

оператор-державний орган, муніципальний орган, юридична або фізична особа, самостійно або спільно з іншими особами організуючі і (або) здійснюють обробку персональних даних, а також визначають цілі обробки персональних даних, склад персональних даних, що підлягають обробці, дії (операції), що здійснюються з персональними даними;

персональні дані-будь-яка інформація, що відноситься до прямо або побічно визначеному або визначається фізичній особі (суб'єкту персональних даних);
надання персональних даних-дії, спрямовані на розкриття персональних даних певній особі або певному колу осіб;
поширення персональних даних – дії, спрямовані на розкриття персональних даних невизначеному колу осіб (передача персональних даних) або на ознайомлення з персональними даними необмеженого кола осіб, у тому числі оприлюднення персональних даних у засобах масової інформації, розміщення в інформаційно-телекомунікаційних мережах або надання доступу до персональних даних будь-яким іншим способом;
транскордонна передача персональних даних-передача персональних даних на територію іноземної держави органу влади іноземної держави, іноземній фізичній або іноземній юридичній особі;
знищення персональних даних-дії, в результаті яких неможливо відновити зміст персональних даних в інформаційній системі персональних даних і (або) в результаті яких знищуються матеріальні носії персональних даних.
Дія Положення поширюється на всі структурні підрозділи Оператора.
Це положення має бути доведено до кожного працівника Оператора, що здійснює обробку персональних даних, під розпис.

2 СУБ'ЄКТИ ТА ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Цілі обробки персональних даних, підстави для їх обробки, можливі дії (операції), що здійснюються з персональними даними, терміни обробки і склад оброблюваних персональних категорій суб'єктів персональних даних, оброблюваних у Оператора, вказані в переліку оброблюваних персональних даних.

3 ОРГАНІЗАЦІЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.1 призначення відповідальних осіб

Для організації обробки персональних даних у Оператора призначається відповідальна особа.
Для визначення рівня захищеності інформаційних систем персональних даних, перевірки готовності засобів захисту інформації до використання, а також знищення персональних даних наказом керівника Оператора призначається комісія з приведення у відповідність до вимог законодавства України в галузі персональних даних (далі – комісія).
У своїй роботі Комісія керується Положенням про Комісію з приведення у відповідність до вимог законодавства України в галузі персональних даних, затвердженим наказом керівника Оператора.

3.2 Допуск працівників до обробки персональних даних

Допуск працівників Оператора до обробки персональних даних здійснюється на підставі наказу про призначення на посаду відповідно до Переліку посад і третіх осіб, які мають доступ до персональних даних.
Працівники Оператора отримують доступ до обробки персональних даних для виконання ними службових (трудових) обов'язків, після виконання наступних заходів:
- ознайомлення під розпис з керівними документами Оператора та нормативними актами України щодо обробки та забезпечення безпеки персональних даних;
- оформлення письмового зобов'язання про нерозголошення персональних даних, форма якого затверджена наказом керівника Оператора.

Працівники Оператора, які мають допуск до персональних даних, мають право отримувати тільки ті персональні дані, які необхідні їм для виконання службових (трудових) обов'язків.
3.3 отримання персональних даних
Персональні дані суб'єкта виходять від нього самого або від нього законного представника. У разі, якщо персональні дані отримані не від суб'єкта персональних даних, Оператор до початку обробки таких персональних даних зобов'язаний повідомити суб'єкт про отримання його персональних даних.
3.4 систематизація, накопичення, уточнення та використання персональних даних
Систематизація, накопичення, уточнення та використання персональних даних здійснюється шляхом оформлення та ведення документів обліку та баз даних суб'єктів персональних даних.
Працівники Оператора, які мають доступ до персональних даних, повинні забезпечити їх обробку, що виключає несанкціонований доступ до них третіх осіб.
3.5 Передача персональних даних
Передача персональних даних суб'єктів третім особам може здійснюватися тільки при наявності письмової згоди суб'єкта, якщо інше не передбачено федеральним законодавством.
При передачі персональних даних суб'єктів третім особам, з третьою особою має бути підписана Угода про дотримання безпеки персональних даних, переданих на обробку, форма якої затверджена наказом керівника Оператора.
Передача персональних даних суб'єктів між підрозділами Оператора повинна здійснюватися тільки між працівниками, допущеними до обробки персональних даних.
3.6 зберігання персональних даних
Зберігання персональних даних суб'єктів здійснюється на паперових і машинних носіях інформації в спеціально виділених сховищах підрозділів Оператора, а також в інформаційних системах Оператора, що забезпечують збереження персональних даних і їх захист від несанкціонованого доступу.
Знищення персональних даних в інформаційних системах, на машинних і паперових носіях інформації повинно проводитися протягом тридцяти днів з дати досягнення мети обробки (граничного терміну зберігання) персональних даних. При неможливості знищення персональних даних протягом тридцяти днів з дати досягнення мети обробки персональних даних, забезпечується їх блокування і знищення в термін, що не перевищує шести місяців.
Порядок і правила обліку, зберігання і знищення персональних даних описані в Регламенті з обліку, зберігання і знищення носіїв персональних даних.
3.7 повідомлення про обробку персональних даних
Згідно із законодавством Оператор повідомляє уповноважений орган із захисту прав суб'єктів персональних даних про обробку персональних даних.
У разі зміни відомостей, зазначених у повідомленні, а також у разі припинення обробки персональних даних Оператор також повідомляє про це уповноважений орган.

4. ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ, ЗДІЙСНЮВАНОЇ БЕЗ ВИКОРИСТАННЯ ЗАСОБІВ АВТОМАТИЗАЦІЇ

Персональні дані при їх обробці без використання засобів автоматизації відокремлюються від іншої інформації шляхом фіксації їх на окремих матеріальних носіях персональних даних, у спеціальних розділах або на полях форм (бланків).
При фіксації персональних даних на матеріальних носіях не допускається запис на одному матеріальному носії персональних даних, цілі обробки яких свідомо несумісні. При

обробці різних категорій персональних даних без використання засобів автоматизації для кожної категорії персональних даних повинен використовуватися окремий матеріальний носій.
При використанні типових форм документів, характер інформації в яких передбачає або допускає включення в них персональних даних, повинні дотримуватися наступні умови:
- типова форма повинна містити відомості про мету обробки персональних даних, найменування та адресу Оператора, прізвище, ім'я, по батькові та адресу суб'єкта персональних даних, джерело отримання персональних даних, терміни обробки персональних даних, перелік дій з персональними даними, які будуть відбуватися в процесі їх обробки, загальний опис використовуваних оператором способів обробки персональних даних;
- типова форма повинна передбачати поле, в якому суб'єкт персональних даних може поставити відмітку про свою згоду на обробку персональних даних - при необхідності отримання письмової згоди на обробку персональних даних;
- типова форма повинна бути складена таким чином, щоб кожен із суб'єктів персональних даних, що містяться в документі, мав можливість ознайомитися зі своїми персональними даними, що містяться в документі, не порушуючи прав і законних інтересів інших суб'єктів персональних даних;
- типова форма повинна виключати об'єднання полів, призначених для внесення персональних даних, цілі обробки яких свідомо не сумісні.
При несумісності цілей обробки персональних даних, зафіксованих на одному матеріальному носії, якщо матеріальний носій не дозволяє здійснювати обробку персональних даних окремо від інших зафіксованих на тому ж носії персональних даних, повинні бути вжиті заходи щодо забезпечення роздільної обробки персональних даних.
Необхідно забезпечувати роздільне зберігання персональних даних (матеріальних носіїв), обробка яких здійснюється в різних цілях.
Знищення або знеособлення частини персональних даних, якщо це допускається матеріальним носієм, може проводитися способом, що виключає подальшу обробку цих персональних даних зі збереженням можливості обробки інших даних, зафіксованих на матеріальному носії.
Уточнення персональних даних при їх обробці без використання засобів автоматизації проводиться шляхом оновлення або зміни даних на матеріальному носії, а якщо це не допускається технічними особливостями матеріального носія, – шляхом фіксації на тому ж матеріальному носії відомостей про внесені в них зміни або шляхом виготовлення нового матеріального носія з уточненими персональними даними.
Особи, які здійснюють обробку персональних даних без використання засобів автоматизації, повинні бути проінформовані:
- про факт обробки ними персональних даних, обробка яких здійснюється без використання засобів автоматизації;
- про категорії оброблюваних персональних даних;
- про особливості та правила здійснення такої обробки.

5 ОРГАНІЗАЦІЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Персональні дані обробляються у Оператора як з використанням засобів автоматизації, так і без використання таких засобів.
Порядок обробки та захисту персональних даних в інформаційних системах Оператора визначається Положенням про забезпечення безпеки персональних даних.

Захист персональних даних від неправомірного їх використання або втрати забезпечується Оператором за рахунок власних коштів.
Працівники Оператора, які в рамках виконання посадових обов'язків мають доступ до персональних даних, зобов'язані дотримуватися режиму конфіденційності персональних даних на всіх етапах їх обробки.
За відсутності працівника на його робочому місці не повинно бути документів і машинних носіїв інформації, що містять персональні дані.
Доступ працівників Оператора та інших осіб в приміщення, в яких здійснюється обробка і зберігання персональних даних, обмежується організаційними заходами і застосуванням системи контролю і управління доступом.
Враховуючи масовість і єдині місця обробки і зберігання, гриф «конфіденційно» на документах, що містять персональні дані, не ставиться.
Організацію обробки персональних даних суб'єктів, контроль дотримання заходів їх захисту в структурних підрозділах Оператора, співробітники яких мають доступ до персональних даних, здійснюють їх безпосередні керівники.
Заходи щодо захисту персональних даних здійснюються відповідно до Плану заходів щодо приведення у відповідність до вимог законодавства України в галузі персональних даних, що затверджуються керівником Оператора.
Розробка та здійснення заходів щодо забезпечення безпеки персональних даних, що обробляються в інформаційних системах, може здійснюватися сторонніми організаціями на договірній основі, що мають ліцензії на право проведення відповідних робіт.

6 ПОРЯДОК ОБРОБКИ ЗВЕРНЕНЬ ТА ЗАПИТІВ З ПИТАНЬ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Порядок обробки запитів суб'єктів персональних даних описаний в Регламенті щодо реагування на запити суб'єктів персональних даних.
Порядок обробки запитів уповноважених органів у галузі персональних даних описаний у Регламенті щодо взаємодії з органами державної влади в галузі персональних даних.

7. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Інші права та обов'язки працівників, у функції яких входить обробка персональних даних, визначаються інструкцією користувача інформаційних систем персональних даних.
Особи, винні в порушенні норм, що регулюють обробку і захист персональних даних, несуть матеріальну, дисциплінарну, адміністративну, цивільно-правову або кримінальну відповідальність в порядку, встановленому федеральними законами.
Розголошення персональних даних, їх публічне розкриття, втрата документів та інших носіїв, які містять персональні дані, а також інші порушення обов'язків щодо їх захисту та обробки, встановлених цим Положенням, іншими локальними нормативними актами (наказами, розпорядженнями) Оператора, тягне накладення на працівника, що має доступ до персональних даних, дисциплінарного стягнення – зауваження, догани, звільнення.
Працівник, який має доступ до персональних даних і вчинив зазначений дисциплінарний проступок, несе повну матеріальну відповідальність у разі заподіяння його діями шкоди роботодавцю.
Працівники Оператора, які мають доступ до персональних даних, винні в їх незаконному розголошенні або використанні без згоди суб'єктів персональних даних з корисливої або іншої особистої зацікавленості і заподіяли велику шкоду, несуть кримінальну відповідальність відповідно до законодавства України.

Оновлення та актуалізація цього Положення здійснюється відповідно до регламенту з проведення контрольних заходів та реагування на інциденти інформаційної безпеки.