УПОВНОВАЖЕНИЙ
ВЕРХОВНОЇ РАДИ УКРАЇНИ
З ПРАВ ЛЮДИНИ

UKRAINIAN
PARLIAMENT COMMISSIONER
FOR HUMAN RIGHTS

вул. Інститутська, 21/8
01008, м. Київ, Україна

Tel.: (+380 44) 253 2203
Fax.:(+380 44) 226 3427
E-mail: hotline@ombudsman.gov.ua
http:// www.ombudsman.gov.ua

21/8, Instytutska str.
Kyiv, 01008, Ukraine

№ _____ «_____»_____ 20 ___ р.

Народному депутату України

Тарасенку Т.П.

Шановний Тарасе Петровичу!

За результатами розгляду Вашого депутатського запиту від 03.02.2020 № 39/20, який надійшов до Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений) разом з листом Голови Верховної Ради України Разумкова Д.О. від 07.02.2020 № 11/10-53 (вх. № 1200/1/20 від 11.02.2020), щодо надання інформації про вжиті заходи у сфері захисту персональних даних повідомляю.

Щодо розробленого проєкту нової редакції Закону України «Про захист персональних даних» (далі – законопроєкт)

Відповідно до Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затвердженого постановою Кабінету Міністрів України від 25.10.2017 № 1106, передбачено завдання щодо удосконалення законодавства про захист персональних даних з метою приведення його у відповідність до Регламенту (ЄС) 2016/679.

Одним із заходів на виконання зазначеного завдання є розроблення та подання на розгляд Кабінету Міністрів України законопроєкту щодо внесення відповідних змін до Закону України «Про захист персональних даних». Відповідальним за виконання цього заходу визначено, зокрема, Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений).

Згідно із Законом України «Про захист персональних даних» Уповноважений має повноваження звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо

прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних.

З огляду на зазначене та для врахування позиції зацікавлених державних органів наказом Уповноваженого від 12.11.2019 № 107.15/19 при Секретаріаті Уповноваженого створено міжвідомчу робочу групу з розроблення законодавчих пропозицій у сфері захисту персональних даних та напрацьовано законопроєкт з урахуванням основних положень Регламенту (ЄС) 2016/679.

У додатку до листа від 17.02.2020 № 992.2/20/26.1 Секретаріату Уповноваженого законопроєкт направлено на розгляд Голові Комітету Верховної Ради України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій у Донецькій, Луганській областях та Автономної Республіки Крим, міста Севастополя, національних меншин і міжнаціональних відносин, народному депутату України Лубінцю Д.В. для прийняття рішення як суб'єкта законодавчої ініціативи (копія листа та законопроєкту додається).

Щодо фінансування Секретаріату Уповноваженого для виконання своїх повноважень

Відповідно до статті 12 Закону України «Про Уповноваженого Верховної Ради України з прав людини» фінансування діяльності Уповноваженого провадиться за рахунок Державного бюджету України та щорічно передбачається в ньому окремим рядком.

Згідно зі статтею 10 зазначеного Закону для забезпечення діяльності Уповноваженого утворюється Секретаріат. З метою реалізації повноважень Уповноваженого в сфері захисту персональних даних у структурі Секретаріату утворено Департамент у сфері захисту персональних даних, працівниками якого в рамках вказаної міжвідомчої робочої групи розроблено законопроєкт.

Додатково на розроблення законопроєкту кошти Державного бюджету України не виділялись, оскільки його було розроблено в рамках поточної діяльності Секретаріату Уповноваженого.

Щодо вжитих заходів контролю за додержанням законодавства про захист персональних даних

У 2018 році у сфері захисту персональних даних:

розглянуто 806 звернень фізичних та юридичних осіб;

складено 14 протоколів про адміністративне правопорушення, з яких 1 протокол згідно з частиною другою статті 188-39 Кодексу України про адміністративні правопорушення (далі – КУпАП), 11 протоколів згідно з частиною четвертою статті 188-39 КУпАП та 2 протоколи згідно зі статтею 188-40 КУпАП;

за наявною інформацією за результатами розгляду судами 2 протоколів, об'єднаних в одне провадження у справі про адміністративне правопорушення, накладено адміністративне стягнення (штраф), 9 проваджень судами закрито у зв'язку із закінченням на момент розгляду

справи строків, передбачених статтею 38 КУпАП, а також 3 провадження закрито у зв'язку з відсутністю складу адміністративного правопорушення;

за результатами перевірок видано 45 приписів про усунення порушень вимог законодавства у сфері захисту персональних даних.

Кількість працівників, які станом на грудень 2018 року займалися питаннями захисту персональних даних – 15 осіб.

Протягом 2019 року у сфері захисту персональних даних:

розглянуто 896 звернень фізичних та юридичних осіб;

складено та передано до суду 9 протоколів про адміністративне правопорушення згідно з частиною четвертою статті 188-39 КУпАП;

за наявною інформацією за результатами розгляду судами 3 протоколів накладено адміністративне стягнення (штраф), 3 протоколи повернуто, 1 провадження судом закрито у зв'язку із закінченням на момент розгляду справи строків, передбачених статтею 38 КУпАП, 1 провадження закрито у зв'язку з відсутністю складу адміністративного правопорушення, а також 1 провадження перебуває на розгляді в суді.

Також уповноваженими посадовими особами Департаменту у сфері захисту персональних даних перевірено 36 володільців/розпорядників персональних даних, з них 27 планових, 5 позапланових перевірок та здійснено 4 моніторингові візити.

За результатами таких перевірок/моніторингових візитів складено 32 акта перевірок додержання законодавства про захист персональних даних, керівникам суб'єктів моніторингу направлено 3 звіти. Відповідно до виявлених порушень володільцям/розпорядникам персональних даних видано для обов'язкового виконання 23 приписи про усунення порушень вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки.

Кількість працівників, які станом на грудень 2019 року займалися питаннями захисту персональних даних – 19 осіб.

Щодо виконання володільцями та розпорядниками персональних даних рекомендацій, наданих у щорічній доповіді Уповноваженого у 2019 році

Відповідно до статті 18 Закону України «Про Уповноваженого Верховної Ради України з прав людини» щорічна доповідь повинна містити посилання на випадки порушень прав і свобод людини і громадянина, щодо яких Уповноважений уживав необхідних заходів, на результати перевірок, що здійснювалися протягом року, висновки та рекомендації, спрямовані на поліпшення стану забезпечення прав і свобод людини і громадянина.

Отже, вказані у щорічній доповіді Уповноваженого висновки надаються за результатами вжиття заходів протягом року (перевірок, розгляду звернень тощо), а тому носять рекомендаційний характер, тобто не містять обов'язку інформування про їх виконання.

Щодо інформації про проведені заходи з інформування про законодавство у сфері захисту персональних даних та вивчення нових практик у цій сфері

Відповідно до пунктів 11, 12 частини першої статті 23 Закону України «Про захист персональних даних» Уповноважений інформує про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними, а також здійснює моніторинг нових практик, тенденцій і технологій захисту персональних даних.

Такі заходи є напрямами поточної діяльності Уповноваженого та Секретаріату Уповноваженого, а тому додаткові бюджетні кошти на них з державного бюджету не виділялися.

Працівниками Секретаріату Уповноваженого у 2018–2019 роках регулярно проводились тренінги, семінари, круглі столи та робочі зустрічі з метою інформування про законодавство у сфері захисту персональних даних. Зокрема, у 2019 році працівниками Секретаріату Уповноваженого та регіональними координаторами у всіх регіонах проведено 31 просвітницький захід.

Також з просвітницькою метою на офіційному веб-сайті Уповноваженого та у Facebook регулярно розміщуються роз'яснення про найбільш поширені та актуальні запитання у сфері захисту персональних даних.

Крім того, працівниками Секретаріату постійно здійснюється моніторинг нових практик, тенденцій і технологій захисту персональних даних. Зокрема, у 2017–2019 роках реалізовано проєкт Twinning Ombudsman «Впровадження кращого європейського досвіду з метою посилення інституційного потенціалу Секретаріату Уповноваженого Верховної Ради України з прав людини для захисту прав і свобод людини», одним із ключових питань якого була сфера захисту персональних даних. Вказаний проєкт фінансувався Європейським Союзом у рамках Європейського інструменту сусідства (ЄІС).

Основними напрямами проєкту були: удосконалення нормативно-правової бази; розроблення методологій, рекомендацій і процедур моніторингу за дотриманням прав і свобод людини; удосконалення інструментів для відновлення порушених прав; впровадження системи тренінгів поглибленого рівня для працівників Секретаріату Уповноваженого на основі кращих європейських практик.

Додаток: на 34 арк. в 1 прим.

З повагою
Уповноважений **Л. Денісова**

УПОВНОВАЖЕНИЙ
ВЕРХОВНОЇ РАДИ УКРАЇНИ
З ПРАВ ЛЮДИНИ

UKRAINIAN
PARLIAMENT COMMISSIONER
FOR HUMAN RIGHTS

вул. Інститутська, 21/8
01008, м. Київ, Україна

Tel.: (+380 44) 253 2203
Fax.:(+380 44) 226 3427
E-mail: hotline@ombudsman.gov.ua
http:// www.ombudsman.gov.ua

21/8, Instytutska str.
Kyiv, 01008, Ukraine

№ _____ «_____»_____ 20 ___ р.

Голові Комітету Верховної Ради України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій у Донецькій, Луганській областях та Автономної Республіки Крим, міста Севастополя, національних меншин і міжнаціональних відносин, народному депутату України

Лубінцю Д.В.

Шановний Дмитре Валерійовичу!

Відповідно до Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 року № 1106, передбачено завдання щодо удосконалення законодавства про захист персональних даних з метою приведення його у відповідність до Регламенту (ЄС) 2016/679.

Одним із заходів на виконання зазначеного завдання є розроблення та подання на розгляд Кабінету Міністрів України законопроєкту щодо внесення відповідних змін до Закону України «Про захист персональних даних». Відповідальним за виконання цього заходу визначено, зокрема, Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений).

Відповідно до Закону України «Про захист персональних даних» Уповноважений має повноваження звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних, інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування та здійснювати моніторинг нових практик, тенденцій і технологій захисту персональних даних.

З огляду на зазначене при Секретаріаті Уповноваженого було створено міжвідомчу робочу групу з розроблення законодавчих пропозицій у сфері захисту персональних даних та напрацьовано проєкт нової редакції Закону України «Про захист персональних даних» з урахуванням основних положень Регламенту (ЄС) 2016/679.

10 лютого 2020 року в Офісі Ради Європи в Україні відбулась зустріч за участю Олени Литвиненко, заступниці Голови Офісу Ради Європи в Україні, Вікторії Гальпєріної, керівниці проєкту, народних депутатів України Тараса Тарасенка та Єгора Чернєва, а також представника Уповноваженого Інни Берназюк, щодо узгодження позицій стосовно проєкту закону «Про захист персональних даних».

За підсумками обговорення вношу Вам на розгляд проєкт закону «Про захист персональних даних», розроблений в Секретаріаті Уповноваженого, для прийняття рішення як суб'єкта законодавчої ініціативи.

У разі доопрацювання цього законопроєкту прошу включити мене та представників Секретаріату Уповноваженого, згідно з додатком, до складу робочої групи.

Додатки:
1. Проєкт закону «Про захист персональних даних»;
2. Список представників від Секретаріату Уповноваженого.

З повагою
Уповноважений **Л. Денісова**

Проєкт

станом на 9:00, 17.02.2020

Закон України

Про захист персональних даних

Цей Закон визначає правові та організаційні засади обробки та захисту персональних даних і спрямований на захист прав людини і основоположних свобод, зокрема права на невтручання в особисте і сімейне життя, у зв'язку з обробкою персональних даних.

Розділ I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Сфера дії Закону

1. Цей Закон поширюється на відносини, пов'язані з обробкою персональних даних, яка здійснюється на матеріальних носіях та/або відображена в електронному вигляді із застосуванням автоматизованих та/або неавтоматизованих засобів.

2. Дія цього Закону поширюється на всіх суб'єктів, які здійснюють обробку персональних даних, незалежно від їхньої організаційно-правової форми чи форми власності, у тому числі, на фізичних осіб.

3. Дія цього Закону не поширюється на обробку персональних даних фізичними особами для особистих чи побутових потреб, які не пов'язані зі здійсненням професійної чи будь-якої іншої діяльності, що має на меті отримання прибутку.

4. Обробка персональних даних для особистих чи побутових потреб охоплює, зокрема, ведення кореспонденції та збереження адрес, підтримання соціальних контактів, а також активність у мережі Інтернет, яка здійснюється в контексті такої діяльності.

5. Вимоги щодо захисту персональних даних не поширюються на обробку:

1) відомостей, що не стосуються ідентифікованої фізичної особи чи фізичної особи, яка може бути ідентифікована;

2) персональних даних знеособлених у спосіб, що унеможливлює ідентифікацію фізичної особи в момент обробки та після такої обробки;

3) відомостей про здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень, відповідно до закону.

Стаття 2. Визначення термінів

1. У цьому Законі терміни вживаються в такому значенні:

персональні дані — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

володілець персональних даних — будь-яка фізична або юридична особа, яка самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних, крім випадків, коли такі цілі визначені законом; володільцем персональних даних також можуть бути громадські організації, які функціонують без створення юридичної особи та громадські ради при органах виконавчої влади;

розпорядник персональних даних - будь-яка фізична або юридична особа, якій володільцем персональних даних або законом надано право обробляти персональні дані від імені володільця;

одержувач - фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа;

суб'єкт персональних даних — фізична особа, персональні дані якої обробляються;

третя особа — будь-яка фізична або юридична особа, за винятком суб'єкта персональних даних, володільця персональних даних, розпорядника персональних даних, а також їхніх працівників, які уповноважені обробляти персональні дані під безпосереднім керівництвом такого володільця або розпорядника персональних даних;

згода на обробку персональних даних — свідоме, вільне, конкретне, інформоване та однозначне волевиявлення суб'єкта персональних даних, виражене у формі заяви та/або чіткої стверджувальної дії, якими він дозволяє обробку своїх персональних даних;

обробка персональних даних — будь-яка дія або сукупність дій з персональними даними з використанням або без використання автоматизованих засобів, зокрема, пошук, збирання, накопичення, структурування, упорядкування, реєстрація, зберігання, організація, ознайомлення, аналіз, профілювання, адаптація, комбінування, зміна, поновлення, використання, поширення (в тому числі розповсюдження, продаж, передача, обмін) або надання доступу іншим чином, обмеження, розмежування, псевдонімізація, знеособлення, вилучення, стирання, знищення, здійснення будь-яких логічних чи арифметичних операцій з такими даними не обмежуючись переліченим;

знеособлення персональних даних - вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу.

порушення цілісності персональних даних - незаконна зміна/поновлення/знищення (повне або часткове) персональних даних;

витік персональних даних — порушення вимог щодо захисту персональних даних, що призвело до випадкового або навмисного неправомірного розкриття або несанкціонованого доступу до персональних даних;

профілювання (створення профілю) — різновид обробки (у тому числі автоматизованої) сукупності (масивів) персональних даних, які вказують або можуть вказувати на певні індивідуальні/особистісні особливості фізичної особи (спосіб життя, інтереси, звички, уподобання тощо), зокрема з метою передбачення варіантів (моделей) її поведінки у майбутньому, пропонування такій особі персоналізованих інформаційних повідомлень (у тому числі рекламних), персоналізованих результатів пошукових запитів, персоналізованих товарів/робіт/послуг тощо.

цифрове профілювання — є різновидом профілювання, в процесі якого здійснюється автоматизована обробка таких персональних даних, як мережеві (щодо телекомунікаційних мереж) та/або інші ідентифікатори фізичної особи, наявність та/або створення яких передбачено умовами використання відповідних пристроїв/приладів, програмних засобів/додатків/розширень та протоколів (зокрема IP-адреси, ідентифікатори типу кукі-файли, дані геолокації, мітки радіочастотної ідентифікації тощо).

біометричні дані — відомості або сукупність відомостей про вимірювані ідентифікуючі фізіологічні характеристики та параметри фізичної особи, зібрані шляхом їх обміру та фіксації

психометричні дані - відомості або сукупність відомостей про психологічні і когнітивні характеристики та параметри фізичної особи, які надають унікальну інформацію про психологічний стан фізичної особи, властивості її психіки, особливості її характеру та темпераменту, психічне здоров'я тощо;

генетичні дані — персональні дані, що стосуються вроджених або набутих генетичних ознак фізичної особи, які надають унікальну інформацію про фізіологію чи здоров'я такої фізичної особи;

ідентифікована фізична особа – фізична особа, яка однозначно виокремлена серед інших фізичних осіб;

фізична особа, яка може бути (конкретно) ідентифікована – особа, яку можна прямо чи опосередковано ідентифікувати, зокрема, з використанням таких ідентифікаторів як ім'я; ідентифікаційний номер; відомості про місцезнаходження; ідентифікатори у мережі Інтернет або у будь-якій інформаційній та/або телекомунікаційній системі; або завдяки одній або декільком ознакам, що є характерними для фізичної, психологічної, генетичної, розумової, економічної, світоглядної, культурної або соціальної ідентичності зазначеної фізичної особи;

картотека персональних даних — будь-які структуровані за певними критеріями персональні дані, обробка яких здійснюється не автоматизовано;

файлова система - структурований набір даних, упорядкованих і доступних за конкретними критеріями;

каталог файлової системи - детальний опис структури і змісту файлової системи;

реєстр каталогів файлових систем - реєстр, що забезпечує детальний облік наявних каталогів файлових систем;

кукі-файли (cookie files) — файли з інформацію у вигляді текстових та/або цифрових даних, які зберігаються у браузері чи на обладнанні суб'єкта персональних даних та містить у собі персональні дані;

псевдонімізація — різновид обробки персональних даних, який полягає у вилученні прямого зв'язку персональних даних з суб'єктом персональних даних та створенням зв'язку між псевдонімом за яким неможливо відтворити зв'язок з суб'єктом персональних даних, без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо із вжиттям всіх необхідних технічні та організаційних заходів захисту;

унікальні персональні дані - персональні дані, які одноразово присвоюються суб'єкту персональних даних та є незмінними з моменту присвоєння (реєстраційний номер облікової картки платника податків, унікальний номер запису в Єдиному державному демографічному реєстрі тощо);

представник - законний або належним чином уповноважений представник суб'єкта персональних або суб'єктів обробки персональних даних;

Уповноважений орган - (???)центральний орган виконавчої влади зі спеціальним статусом, що забезпечує формування та реалізацію державної політики у сфері захисту персональних даних, та уповноважений на здійснення функцій нагляду і контролю у відповідній сфері. (???)

Стаття 3. Законодавство про захист персональних даних

Законодавство про захист персональних даних складають Конституція України, цей Закон, інші закони та підзаконні нормативно-правові акти, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 4. Загальні вимоги до обробки та захисту персональних даних

1. Обробка персональних даних володільцем персональних даних не допускається, якщо досягнення поставлених цілей можливе без такої обробки.

Персональні дані можуть оброблятися в формі, яка дозволяє ідентифікувати суб'єкта даних, лише у тих випадках, якщо обробка даних в знеособленому вигляді не дозволяє досягти визначеної мети такої обробки.

2. Особа, яка обробляє персональні дані, зобов'язана обробляти такі дані:

виключно за наявності чітких правових підстав;

з конкретно визначеною метою, сформульованою в документах, які регулюють діяльність володільця, та/або визначеною в законах, інших нормативно-правових актах з урахуванням вимог, встановлених законодавством про захист персональних даних;

відкрито і прозоро із застосуванням процесів та засобів, що відповідають визначеним цілям (меті) обробки;

із застосуванням процесів та засобів, суть яких може бути описана (пояснена) володільцем та/або розпорядником загальнодоступними для сприйняття засобами;

не довше ніж це необхідно для цілей, з якими персональні дані були зібрані.

3. Володілець персональних даних зобов'язаний визначити мету обробки персональних даних до початку їх збору та не може змінювати її після збору персональних даних без згоди суб'єктів персональних даних, крім випадків, передбачених законом.

4. Володілець зобов'язаний дотримуватись таких вимог щодо складу, обсягу та змісту персональних даних, які ним обробляються:

персональні дані повинні бути адекватними, відповідними і ненадмірними відповідно до визначеної мети їх обробки, не допускається збір та обробка персональних даних у кількості, що є надмірною відповідно до визначеної мети;

персональні дані повинні бути точним, достовірними та підтримуватися в актуальному стані;

5. Захист персональних даних забезпечується шляхом впровадження та реалізації відповідних технічних і організаційних заходів, зокрема:

псевдонімізації та шифрування персональних даних;

забезпечення конфіденційності, цілісності, доступності і стійкості систем і сервісів обробки;

забезпечення своєчасного відновлення доступності персональних даних у разі виникнення фізичного або технічного інциденту;

регулярного тестування, оцінки та вимірювання ефективності технічних та організаційних заходів щодо забезпечення безпеки обробки.

застосування процесів та способів обробки персональних даних (технічних, організаційних заходів тощо), які гарантують їх безпеку, у тому числі, захист від порушення цілісності персональних даних або витоку персональних даних.

6. Володілець персональних даних зобов'язаний застосовувати належні організаційні та технічні заходи для того, щоб здійснювалась обробка лише тих персональних даних, обробка яких є необхідною для кожної конкретної цілі обробки. Цей обов'язок володільця стосується обсягу персональних даних, які збираються, способу їх обробки, періоду, протягом якого дані зберігаються та залишаються доступними.

7. Володілець персональних даних зобов'язаний вжити усі належні організаційні та технічні заходи щодо виконання вимог цього Закону до початку обробки персональних даних та підтримувати їх актуальність під час такої обробки.

8. Обов'язок доведення факту додержання вимог цієї статті покладається на володільця персональних даних. Володілець персональних даних зобов'язаний вжити заходи, які забезпечуватимуть можливість підтвердження дотримання встановлених цією статтею вимог.

Розділ II

ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ ОБРОБКА

Стаття 5. Відомості, що відносяться до персональних даних

1. До відомостей, що містять або становлять персональні дані належать, зокрема:

1) відомості передбачених законодавством документів, що посвідчують особу - зміст та реквізити таких документів;

2) контактні дані: відомості, які дають можливість зв'язатися з конкретною фізичною особою, або ідентифікувати особу, яка у певний проміжок часу скористалася поштовими, комунікаційними послугами чи іншими послугами;

3) ідентифікатори речей і обладнання, їх складових частин, які перебувають у володінні або користуванні суб'єкта персональних даних, зокрема серійні (заводські) номери, державні номерні знаки;

4) ідентифікатори у мережі Інтернет або у будь-якій інформаційній та/або телекомунікаційній системі до яких, зокрема, відносяться: статичні та динамічні IP адреси (Internet Protocol address), MAC-адреси, інші ідентифікатори;

5) метадані наданих та отриманих послуг, до яких, зокрема, відносяться: відомості про замовників, виконавців, інших осіб, час, місце, обставини, умови надання послуги, у чому вона полягала;

6) відомості про взаємовідносини суб'єкта персональних даних з іншими фізичними особами;

7) відомості про події, обставини, вчинки, які мають безпосереднє відношення до фізичної особи або її характеризують;

8) відомості про юридичні факти, які стосуються суб'єкта персональних даних, до яких, зокрема, відносяться: відносини немайнового та майнового характеру - укладені за участю або на користь суб'єкта персональних даних правочини, права та обов'язки надані/покладені/обмежені нормативно-правовими актами, рішеннями компетентних (у тому числі судових) органів;

9) генетичні дані;

10) біометричні дані, до яких, зокрема, відносяться: відбитки пальців; форма чи пропорції тіла або його частин; малюнок сітківки ока або райдужної оболонки ока; форма чи пропорції обличчя або його частин; теплове зображення тіла або його частин (термограма); статура тіла; хода; рукописний або клавіатурний почерк; зображення фізичної особи або частин її тіла; голос; інші унікальні фізіологічні характеристики, які дають змогу ідентифікувати особу.

11) психометричні дані, до яких, зокрема, відносяться: поведінкові характеристики, характерні звички, схильності, уподобання, звичні форми поведінки або емоційних проявів, особливості когнітивних функцій особи, результати психологічних тестувань та досліджень, дії фізичної особи в мережі Інтернет, історія пошукових запитів та відвідуваних веб-сторінок;

12) відомості про перебування та шляхи пересування фізичних осіб, зокрема дані геолокації тощо;

13) відомості про себе, оприлюднені особою, у тому числі, за допомогою засобів масової інформації, в мережі Інтернет, в соціальних мережах, мессенджерах, блогах тощо;

14) відомості про померлих родичів та/або близьких осіб, необхідні для реалізації прав та законних інтересів суб'єкта персональних або якщо поширення таких відомостей спричинить або може спричинити настання для суб'єкта персональних даних певних правових та/або соціальних наслідків;

15) результати профілювання, а також прийняті на підставі та/або з урахуванням цих результатів рішення.

2. Перелік відомостей що містять або становлять персональні дані, наведений у частині першій цієї статті, не є вичерпним. (Перелік відомостей, що становлять персональні дані не є вичерпним.)

3. Відомості про фізичну особу, що дозволяють однозначно виокремити її серед інших осіб в конкретний проміжок часу вважаються ідентифікуючими персональними даними.

До ідентифікуючих персональних даних за замовчуванням належать відомості про володіння унікальною річчю/об'єктом, про права на таку річ/об'єкт, відомості про речі/об'єкти, права на які зареєстровані в установленому законом порядку, а також унікальні персональні дані.

Стаття 6. Обробка відомостей про фізичну особу, яка може бути ідентифікована

1. Вимоги до обробки та захисту персональних даних, визначені у статті 3 цього Закону, поширюються на обробку будь-яких відомостей про фізичну особу , яка ідентифікована чи може бути конкретно ідентифікована.

2. Якщо обсяг відомостей про фізичну особу, що обробляється володільцем або розпорядником персональних даних, є недостатнім для ідентифікації фізичної особи, проте існують обґрунтовані підстави вважати, що в майбутньому можуть бути одержані додаткові відомості про фізичну особу, які самостійно чи разом із раніше одержаними відомостями забезпечать можливість ідентифікації цієї фізичної особи, на такі відомості про фізичну особу поширюються вимоги до обробки та захисту персональних даних.

3. Для визначення того, чи може фізична особа бути ідентифікована, зокрема в майбутньому, володілець або розпорядник персональних даних повинні враховувати всі розумно можливі способи ідентифікації фізичної особи. До таких способів належить, зокрема, отримання додаткових відомостей про фізичну особу; поєднання, виділення, порівняння різних відомостей про фізичну особи; поєднання, виділення, порівняння відомостей про кількох фізичних осіб.

4. Вимоги частин другої - четвертої цієї статті поширюються на знеособлені або псевдонімізовані персональні дані, якщо вони у поєднанні з іншими відомостями ідентифікують фізичну особу.

Стаття 7. Персональні дані, обробка яких становить особливий ризик порушення прав людини і основоположних свобод

1. До персональних даних, обробка яких становить особливий ризик порушення прав людини і основоположних свобод належать, зокрема, відомості про:

расове, етнічне та національне походження;

політичні, релігійні, світоглядні переконання;

членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;

стан здоров'я;

статеве життя;

біометричні дані;

генетичні дані;

притягнення до адміністративної чи кримінальної відповідальності;

застосування щодо особи заходів в рамках досудового розслідування;

проведення оперативно-розшукових, розвідувальних, контррозвідувальних заходів щодо особи;

випадки насильства щодо особи;

місцеперебування та/або шляхи пересування особи;

соціальні зв'язки та контакти (відносини фізичної особи з іншими особами);

метадані, що стосуються наданих та отриманих телекомунікаційних послуг;

відомості зазначені в пунктах 5, 6, 9 та 10, 11, 12, 15 частини першої статті 4 цього Закону;

відомості щодо активності фізичних осіб отримані в процесі систематичного моніторингу їх взаємодії з навколишнім середовищем та в кіберпросторі.

Стаття 8. Особливі вимоги до обробки персональних даних

1. 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.

2. Положення частини першої цієї статті не застосовується, якщо обробка персональних даних:

1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних, а також у випадках, коли отримання однозначної згоди суб'єкта персональних даних неможливе до початку обробки таких даних через його фізичний/психологічний стан;

4) 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;

5) необхідна для обґрунтування, задоволення або захисту власної правової вимоги;

6) необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються закладом охорони здоров'я чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, центральним органом виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, за умов покладення на працівників зазначених суб'єктів, а також осіб, які від імені цих суб'єктів здійснюють безпосередню обробку персональних даних з передбаченою цим пунктом метою (мають доступ до таких даних тощо), обов'язків щодо забезпечення захисту персональних даних, які стали їм відомі у зв'язку з виконанням професійних або службових обов'язків (дотримання лікарської таємниці);

7) стосується вироків/рішень суду в кримінальних/адміністративних справах, виконання завдань оперативно-розшукової чи розвідувальної/контррозвідувальної діяльності, боротьби з тероризмом, відвернення або подолання наслідків стихійних лих та здійснюється державним органом в межах його повноважень, визначених законом;

8) стосується даних, які були явно оприлюднені суб'єктом персональних даних;

9) здійснюється у випадках прямо передбачених законами України.

Стаття 9. Підстави для обробки персональних даних

1. Підставами для обробки персональних даних є:

1) згода суб'єкта персональних даних на обробку його персональних даних;

2) необхідність здійснення повноважень володільця персональних даних даних, визначених законом;

3) 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;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом;

6) необхідність захисту прав чи законних інтересів володільця, розпорядника персональних даних або третьої особи, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

Стаття 10. Згода суб'єкта персональних даних

1. Згода суб'єкта персональних даних на обробку його персональних даних надається таким суб'єктом шляхом добровільного вчинення чіткої стверджувальної дії, здійсненням якої

суб'єкт персональних даних добровільно та однозначно погоджується на обробку його персональних даних.

Реалізація прав та свобод суб'єкта персональних даних не може залежати від надання суб'єктом згоди на обробку його даних.

2. Згода суб'єкта персональних даних на обробку його персональних даних може бути надана:

1) у формі письмової заяви, анкети, бланку, тощо, в тому числі поданої електронними засобами;

2) в електронній формі під час відвідування веб-сайту або користування електронною інформаційною системою, шляхом заповнення передбаченої інтерфейсом форми, проставлення у відповідному полі відмітки/позначки;

3) шляхом обрання відповідних технічних налаштувань в інтерфейсі веб-сайта, операційній системі, програмному забезпеченні, чи мобільному додатку які передбачають обробку персональних даних;

4) через іншу ствердну дію чи поведінку, яка однозначно вказує на те, що суб'єкт персональних даних у вказаному контексті згоден на подальшу обробку його персональних даних.

3. Не можуть розглядатися в якості згоди суб'єкта персональних даних на обробку його персональних даних:

1) мовчазні та невизначені дії суб'єкта персональних даних;

2) автоматичне заповнення передбаченої інтерфейсом форми або попереднє проставлення у відповідному полі відмітки (позначки) без безпосередньої участі конкретного суб'єкта персональних даних;

3) встановлені за замовчуванням налаштування веб-сайту, операційної системи, програмного забезпечення, мобільного додатку;

4) бездіяльність такого суб'єкта.

4. Згода суб'єкта персональних даних на обробку його персональних даних повинна бути: добровільною, поінформованою, конкретною, змістовною та чіткою.

1) Добровільність згоди

Не допускається примушування суб'єкта персональних даних до надання згоди на обробку його персональних даних, та/або створення умов, за яких у такого суб'єкта буде відсутня можливість вільного вибору щодо надання чи ненадання відповідної згоди.

Не допускається відмова від надання суб'єкту персональних даних товарів чи послуг на підставі відмови суб'єкта від надання згоди, за виключенням випадків, коли надання товарів і послуг неможливе без обробки персональних даних.

Згода не вважається добровільною якщо:

суб'єкт персональних даних знаходиться у залежному чи підпорядкованому становищі відносно особи якій надається згода;

у суб'єкта персональних даних немає вільного вибору або немає можливості відмовити в наданні згоди або немає можливості відкликати раніше надану згоду, без настання негативних наслідків для себе;

у суб'єкта персональних даних відсутні альтернативні шляхи доступу до певних товарів, послуг, соціальних благ тощо, без надання ним згоди на обробку своїх персональних даних.

2) Поінформованість згоди

Згода суб'єкта персональних даних на обробку його персональних даних вважається поінформованою, якщо до її надання або на момент її надання відповідний суб'єкт був проінформований про:

мету, склад, зміст та процедури обробки його персональних даних;

володільця та розпорядника (у випадку наявності) персональних даних, засоби зв'язку з ними (інформація повинна бути надана в такому обсязі щоб суб'єкт персональних даних мав можливість ідентифікувати володільця та розпорядника і міг безперешкодно з ними зв'язатися);

третіх осіб яким передаються чи можуть передаватися його персональні дані, а також про умови такої передачі;

свої права передбачені чинним законодавством України у сфері захисту персональних даних;

способи реалізації своїх права передбачені чинним законодавством України у сфері захисту персональних даних.

3) Конкретність, змістовність та чіткість згоди

Згода суб'єкта персональних даних на обробку його персональних даних повинна:

бути надана на обробку персональних даних з конкретною та зрозумілою для відповідного суб'єкта метою. У разі, якщо обробка персональних даних здійснюється для декількох цілей, згода суб'єкта персональних даних повинна охоплювати кожну з таких цілей обробки.

бути надана на обробку конкретного, чітко визначеного складу та обсягу персональних даних;

охоплювати всі процеси (види) обробки персональних даних, здійснення яких передбачається для досягнення конкретної мети або декількох конкретно сформульованих цілей.

5. Згода на обробку персональних надається (адресується) володільцю персональних даних незалежно від форм та способів її надання, а також осіб, що здійснюють її фактичне отримання.

6. Недотримання вимог щодо згоди суб'єкта персональних даних на обробку його персональних даних, встановлених цією статтею, тягне за собою недійсність такої згоди з моменту її надання.

7. Обов'язок доведення факту надання суб'єктом персональних даних згоди на обробку його даних покладається на володільця персональних даних. Володілець персональних даних зобов'язаний забезпечити такі процедуру, механізм та порядок надання згоди, які передбачатимуть можливість підтвердження дотримання встановлених цією статтею вимог до згоди суб'єкта персональних даних на обробку його персональних даних.

8. Обробка персональних даних державними органами, органами місцевого самоврядування, суб'єктами природних монополій, а також підприємствами, установами або організаціями, які здійснюють владні повноваження, здійснюється виключно на підставі пунктів 2 - 6 частини першої статті 8 цього Закону.

9. Якщо обробка персональних даних здійснюється на підставі згоди суб'єкта персональних даних, відповідний суб'єкт має право відкликати згоду в будь-який момент. Відкликання згоди не повинно впливати на законність обробки, що ґрунтувалася на згоді до її відкликання. Володілець персональних даних повинен однаково забезпечити суб'єкту персональних даних можливість як відкликати, так і надати згоду.

Стаття 11. Обробка біометричних даних державними органами та органами місцевого самоврядування

1. Обробка біометричних даних державними органами та органами місцевого самоврядування як володільцями персональних даних допускається виключно з метою:

1) забезпечення національної безпеки, оперативно-розшукової та контррозвідувальної діяльності, протидії злочинності, підтримання громадської безпеки і порядку, економічного добробуту та прав людини;

2) авторизації користувачів в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, за для уникнення розголошення інформації з обмеженим доступом в процесі виконання покладених на них функцій та повноважень, якщо досягнення зазначених цілей іншими засобами неможливе або пов'язане з непропорційними зусиллями;

3) оформлення в порядку, встановленому законодавством, документів, що посвідчують особу;

4) здійснення в порядку, встановленому законодавством, ідентифікації та верифікації осіб;

5) в інших випадках, прямо передбачених законами України.

Стаття 12. Здійснення відеоспостереження

1. Здійснення відеоспостереження в громадських та публічних місцях, інших територіях загального користування, а також в громадському транспорті, допускається лише в прямо передбачених законом цілях, зокрема з метою попередження правопорушень, забезпечення громадської безпеки.

2. Юридичні та фізичні особи можуть здійснювати відеоспостереження в будівлях (крім житлових) та на територіях, які перебувають у їх власності або законному володінні чи користуванні, в цілях попередження правопорушень, забезпечення громадської безпеки, забезпечення безпеки фізичних осіб та збереження майна, охорони майнових та немайнових прав, забезпечення прозорості діяльності державних та комунальних органів, підприємств, установ та організацій, забезпечення прозорості проведення іспитів та тестувань, публічних конкурсів, контролю доступу до будівель та територій,

Здійснення відеоспостереження, передбаченого частинами першою та другою цієї статті, здійснюється без отримання згоди суб'єкта персональних даних, але за умови повідомлення відповідно до статті __ цього Закону.

3. Здійснення роботодавцем відеоспостереження за працівниками безпосередньо на робочому місці допускається на підставі письмової або прирівняної до неї згоди таких працівників

як суб'єктів персональних даних, наданої з урахуванням вимог цього Закону, виключно з метою організації безпеки працівників, збереження майна та конфіденційної інформації, крім випадків коли інші цілі прямо передбачені законодавством. У разі встановлення відеоспостереження на робочих місцях роботодавець зобов'язаний у письмовій або прирівняної до неї формі проінформувати усіх працівників та інших осіб що можуть перебувати в зоні відеоспостереження, про факт та зони здійснення відеоспостереження, функціональні можливості обладнання для відеоспостереження, а також мету здійснення відеоспостереження, їх правах як суб'єктів персональних даних. Відеозаписи не можуть використовуватись та поширюватись для приниження честі чи гідності особи.

4. Здійснення відеоспостереження не допускається в приміщеннях для зміни одягу, якщо така зміна передбачає повне чи часткове оголення частин тіла які відповідно до існуючих у суспільстві традицій не підлягають оголенню в публічних місцях, а також в місцях, призначених для задоволення гігієнічних чи інших фізіологічних потреб.

5. Відеоспостереження житлових будівель та приміщень допускається виключно з метою забезпечення безпеки фізичних осіб та майна, на підставі письмової згоди більше половини власників такої будівлі або приміщення та за таких умов:

1) системи відеоспостереження може здійснюватися лише шляхом моніторингу входу та загальних приміщень;

2) моніторинг приватних приміщень квартир не допускається;

3) перегляд збережених відеозаписів допускається лише у разі скоєння протиправних дій або посягань на такі дії, з метою встановлення осіб, винних у вчиненні таких дій;

4) використання чи поширення відеозаписів не може здійснюватись для приниження честі чи гідності фізичної особи.

6. У разі встановлення відеоспостереження особи які здійснюють відеоспостереження зобов'язані розміщувати в доступному для огляду місці відповідний попереджувальний знак. У такому випадку суб'єкт персональних даних вважається поінформованим щодо обробки його персональних даних.

7. У разі якщо при здійсненні відеоспостереження відбувається збереження відеозаписів, особа, яка здійснює відеоспостереження, зобов'язана створити файлову систему, призначену для зберігання відеозаписів. Крім відеозаписів (зображення/звук) в системі повинна міститися інформація про дату, місце і час здійснення запису, а також відомості про осіб які переглядали збережені відеозаписи, дату, місце, час та підстави здійснення перегляду відеозапису.

8. Особи, відповідальні за здійснення відеоспостереження, зобов'язані забезпечити захист системи відеоспостереження та її складових і відеозаписів від витоку персональних даних та порушення цілісності персональних даних.

9. В розумінні цього Закону, особа яка здійснює відеоспостереження у власних цілях вважається володільцем персональних даних, а особа яка здійснює відеоспостереження у цілях визначених іншою особою вважається розпорядником персональних даних.

10. Забезпечення захисту системи відеоспостереження, її складових частин, а також персональних даних, що обробляються з її використанням, здійснюється з дотриманням загальних вимог, передбачених цим Законом та іншими нормативно-правовими актами в сфері захисту персональних даних.

11. Вимоги до здійснення відеоспостереження, передбачені цією статтею застосовуються до фотозйомки, яка здійснюється в аналогічний спосіб з такими ж цілями.

Стаття 13. Обробка персональних даних за допомогою веб-сайту

1. Будь-яка обробка персональних даних за допомогою веб-сайту допускається виключно за згодою суб'єкта персональних даних.

2. Факт відвідування веб-сайту суб'єктом персональних даних вважається згодою на обробку його персональних даних, але виключно в обсязі, мінімально необхідному для висвітлення змісту веб-сайту засобами веб-переглядача (браузера). В такому разі допускається лише обробка технічних даних, необхідних для коректного відображення змісту веб-сайту та його взаємодії з веб-переглядачем (браузером) користувача.

3. У тому випадку, якщо функціональні можливості та умови користування веб-сайту передбачають вчинення будь-яких додаткових дій суб'єкта персональних даних, результат яких впливає/може впливати на обсяг його прав та обов'язків або спричинити настання обставин, що мають юридичне значення, за замовчуванням вважається, що засобами такого веб-сайту здійснюється обробка персональних даних в обсязі, необхідному для попереднього отримання згоди на обробку персональних даних від відповідного суб'єкта з урахуванням вимог цього Закону.

3. Положення частини другої цієї статті не застосовуються до обробки персональних даних з будь-якою іншою метою крім висвітлення змісту веб-сайту на веб-переглядачі (браузері).

4. Особа яка обробляє персональні дані засобами веб-сайту зобов'язана надати суб'єкту персональних даних інформацію визначену статтею 18 цього Закону;

5. Ненадання згоди на обробку персональних даних не може бути підставою для обмеження перегляду змісту веб-сайту. В такому разі забороняється обробка будь-яких відомостей крім тих про які йдеться у частині другій цієї статті.

6. Положення цієї статті застосовуються також і до обробки персональних даних веб-сторінкою.

Стаття 14. Використання кукі-файлів

1. Використання кукі-файлів допускається лише на підставі згоди суб'єкта персональних даних, крім тих кукі-файлів, без яких веб-сайт не може функціонувати з технічних причин.

2. При відвідуванні веб-сайту суб'єктом персональних даних і до початку використання кукі-файлів особа яка обробляє персональні дані зобов'язана:

1) поінформувати суб'єкта персональних даних про використання кукі-файлів, їх призначення та функціональні можливості щодо збору персональних даних;

2) запитати суб'єкта персональних даних про згоду на використання кукі-файлів щодо нього та надати можливість суб'єкту персональних даних відмовитися від такого використання.

3. Доступ суб'єкта персональних даних до веб-сайту або його окремих розділів не може бути обмежений через відмову такого суб'єкта від використання кукі-файлів щодо нього.

Стаття 15. Повідомлення Уповноваженого органу про обробку персональних даних

1. Володілець персональних даних повідомляє Уповноважений орган про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки, окрім персональних даних до обробки яких встановлено особливі вимоги.

2. Володілець персональних даних повідомляє Уповноважений орган про намір здійснювати обробку персональних даних до обробки яких встановлено особливі вимоги не пізніше тридцяти робочих днів до початку такої обробки.

3. Володілець персональних даних зобов'язаний повідомляти Уповноважений орган про кожну зміну відомостей, що підлягають повідомленню в такі строки:

стосовно відомостей зазначених у частині першій цієї статті - упродовж десяти робочих днів з дня настання такої зміни;

стосовно відомостей зазначених у частині другій цієї статті - пізніше десяти робочих днів до такої зміни.

4. Види обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, та категорії суб'єктів, на яких поширюється вимога щодо повідомлення, визначаються Уповноваженим органом.

5. Повідомлення про обробку персональних даних та про намір здійснювати обробку персональних даних подається за формою та в порядку, визначеному Уповноваженим органом. Уповноваженим органом також визнається перелік документів які подаються разом із повідомленням про намір здійснювати обробку персональних даних.

6. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого органу в порядку, визначеному Уповноваженим.

Стаття 16. Особливості обробки персональних даних в трудових відносинах

1. Відмова суб'єкта персональних даних від надання згоди на обробку персональних даних не може бути підставою для відмови у працевлаштуванні, звільненні, переведені на іншу посаду.

2. Відмова кандидата на вакантну посаду або працівника, який відповідно до своїх посадових обов'язків повинен мати доступ до персональних даних від взяття на себе зобов'язання щодо нерозголошення персональних даних та належного поводження з ними може бути підставою для відмови у працевлаштуванні, звільненні, переведені на іншу посаду.

3. Суб'єкт персональних даних, який перебуває в трудових відносинах має право безперешкодно знайомитися з матеріалами своєї особової справи, а також робити копії документів які у ній зберігаються. За вимогою такого суб'єкта персональних даних роботодавець, його представники, уповноважені ним особи зобов'язані в установленому порядку засвідчити вірність копій документів, які зберігаються в особовій справі.

4. Матеріали особової справи надаються суб'єкту персональних даних на його усний або письмовий запит, складений у довільній формі, у той самий день, а якщо це неможливо з технічних причин - не пізніше ніж на наступний робочий день з дати звернення із запитом.

Стаття 17. Позначення документів, які містять персональні дані

1.У разі збирання на підставі згоди суб'єкта персональних даних або у випадках прямо передбачених законами України, копії/сканованої копії офіційного документу (документу, що посвідчують особу, довідки про присвоєння ідентифікаційного номера, свідоцтва про факт державної реєстрації акту цивільного стану, військового квитка, посвідчення, перепустки тощо), володілець, розпорядник персональних даних зобов'язаний нанести спеціальні позначки (текстові або графічні знаки) володільця або розпорядника персональних даних.

2.У разі оприлюднення, на підставі згоди суб'єкта персональних даних або у випадках прямо передбачених законами України, документу (його копії, сканованої копії), зокрема у мережі Інтернет, володілець, розпорядник персональних даних зобов'язаний перед оприлюдненням документу нанести спеціальні позначки (текстові або графічні знаки) володільця, розпорядника персональних даних.

3. Спеціальні позначки (текстові або графічні знаки) володільця, розпорядника персональних даних складаються із найменування володільця, розпорядника персональних даних та наносяться на документ (його копію, скановану копію) суцільним напівпрозорим текстом по всьому документу у спосіб, що не дасть змоги їх видалити.

4.Збирання та оприлюднення зазначених документів (їх копій, сканованих копій) без спеціальних позначок (текстових або графічних знаків) володільця, розпорядника персональних даних забороняється.

Розділ ІІІ
ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 18. Надання інформації суб'єкту персональних даних

1. Якщо персональні дані збираються безпосередньо від суб'єкта персональних даних, особа яка збирає персональні дані не пізніше ніж у момент отримання персональних даних зобов'язана повідомити такому суб'єкту інформацію про:

1) володільця персональних даних - його ідентифікаційні та контактні дані;

2) контактні дані особи, відповідальної за захист персональних даних, за умов її призначення відповідно до статті __ цього Закону;

3) цілі обробки та склад персональних даних;

4) правові підстави для обробки персональних даних;

5) осіб, яким передаються/можуть передаватися персональні дані;

6) строк, протягом якого зберігатимуться персональні дані або критерії для його визначення, якщо конкретний строк в момент збору персональних даних визначити неможливо;

7) право подати скаргу до Уповноваженого органу та контактні дані такого органу;

8) форму, зміст та порядок надання/відкликання згоди на обробку персональних даних, якщо обробка таких даних здійснюється на підставі згоди;

9) права суб'єкта персональних даних згідно з цим Законом

10) правові наслідки, пов'язані з наданням/ненаданням, персональних даних;

12) наявність механізму автоматизованого прийняття рішень, у тому числі профілювання і, за наявності такого механізму, — надати необхідну інформацію про алгоритми (логіку), що використовуються у таких механізмах, а також значимість та передбачувані наслідки такої обробки для суб'єкта персональних даних;

13) здійснення обробки персональних даних для цілей прямого маркетингу, а також про право відмовитися від обробки персональних даних для таких цілей

2. Якщо персональні дані збираються не безпосередньо від суб'єкта персональних даних, інформація, передбачена частиною першою цієї статті, а також відомості про джерела отримання персональних даних, повідомляються суб'єкту персональних даних володільцем:

1) якщо персональні дані будуть використовуватися для встановлення контакту з суб'єктом персональних даних — одночасно з першим контактом, або

2) якщо передбачається поширення персональних даних — до першого факту такого поширення,

3) але в будь-якому випадку не пізніше тридцяти днів з моменту збору персональних даних або до моменту їх першого поширення.

3. Положення частини першої та другої цієї статті не застосовується у наступних випадках:

1) суб'єкт персональних даних вже має інформацію зазначену в частині першій цієї статті;

2) надання такої інформації є неможливим у зв'язку з відсутністю контактних даних суб'єкта персональних даних або неможливістю встановити з ним зв'язок з використанням наявних контактних даних;

3) права та обов'язки володільця чи розпорядника щодо збору та/або поширення персональних даних прямо передбачені законодавством України;

4) персональні дані не підлягають розголошенню володільцем персональних даних, якщо таке розголошення спричинить порушення таким володільцем передбаченого законом режиму захисту професійної таємниці, державної таємниці або таємниці досудового розслідування, оперативно-розшукової і контррозвідувальної діяльності та боротьби з тероризмом.

Стаття 19. Право суб'єкта персональних даних на доступ до відомостей про себе

1. Суб'єкт персональних даних має право на доступ шляхом ознайомлення та/або на одержання будь-яких відомостей про себе, в тому числі копій документів, в яких такі відомості містяться, у будь-якої особи, яка обробляє персональні дані відповідного суб'єкта, крім випадків, передбачених законом.

2. З метою отримання відомостей, зазначених в частині першій цієї статті, суб'єкт персональних даних подає запит поштою, електронною поштою, через відповідний електронний кабінет або особисто відповідній особі, яка обробляє персональні дані.

Запит має містити прізвище, ім'я та по батькові, місце проживання (місце перебування), реквізити документа, що посвідчує фізичну особу, яка подає запит, підпис. Якщо запит подається поштою, підпис суб'єкта персональних даних має бути засвідчений нотаріально. У разі подання запиту з використанням інформаційно-телекомунікаційних мереж (електронною поштою тощо) такий запит має бути підписаний кваліфікованим електронним підписом відповідного суб'єкта персональних даних. Запит може бути поданий особисто за умови пред'явлення документу, що посвідчує особу запитувача.

3. Строк надання відповіді на запит щодо доступу до відомостей про себе не може перевищувати 30 календарних днів. Запитувана інформація має надаватись суб'єкту персональних даних за умови вжиття необхідних заходів, що унеможливлюють несанкціонований доступ до персональних даних сторонніх осіб.

Запитувана інформація надається:

особисто, за умови пред'явлення документу, що посвідчує особу запитувача;

шляхом направлення запитуваної інформації засобами поштового зв'язку рекомендованим листом з позначкою на конверті «вручити особисто» на адресу суб'єкта персональних даних з обов'язковим пред'явлення документу, що посвідчує особу запитувача при отриманні листа;

електронною поштою, у разі, якщо електронний запит підписаний кваліфікованим електронним підписом відповідного суб'єкта персональних даних;

через відповідний електронний кабінет за допомогою якого суб'єкт персональних даних є однозначно ідентифікований.

4. Суб'єкт персональних даних має право також особисто ознайомитись із документами у яких містяться відомості про нього за місцем їх зберігання, крім випадків, передбачених законом.

5. У разі, якщо у відомостях чи документах, крім персональних даних запитувача, міститься інформація про інших осіб, то при наданні доступу запитувачу така інформація підлягає знеособленню (закриттю, ретушуванню тощо) у спосіб, що унеможливлює її відтворення та/або зчитування.

6. Доступ суб'єкта персональних даних до відомостей про себе здійснюється безоплатно, крім випадків, передбачених законодавством.

7. Відмова в доступі суб'єкта персональних даних до відомостей про себе допускається, якщо доступ до них заборонено згідно із законом. У повідомленні про відмову зазначаються причини та правові підстави для відмови, а також порядок оскарження рішення про відмову.

8. Рішення про відмову у доступі до персональних даних може бути оскаржено до вищестоящої посадової особи, Уповноваженого органу або суду. Обов'язок доведення законності відмови у доступі покладається на того хто відмовив у доступі.

Стаття 20. Право на видалення персональних даних

1. Суб'єкт персональних даних має право вимагати видалення його персональних даних (у тому числі їх копій та посилань на них) від особи, яка обробляє персональні дані за умов, якщо:

1) такі дані більше не потрібні для досягнення визначеної мети обробки або мета досягнута;

2) відсутні або втратили чинність правові підстави для обробки персональних даних;

3) суб'єкт персональних даних заперечує проти обробки своїх персональних даних відповідно до статті 23 цього Закону;

4) персональні дані повинні бути видалені для виконання обов'язку володільця, який передбачений законом.

2. Якщо обов'язок видалення персональних даних виник щодо персональних даних які були поширені, особа яка, поширила персональні дані зобов'язана повідомити усіх осіб, яким вони були поширені про необхідність видалення таких даних, їх копій та посилань на них.

3. Положення частин першої та другої цієї статті не застосовуються, якщо обробка персональних даних:

1) необхідна для реалізації права на свободу думки і слова на вільне вираження своїх поглядів і переконань у відповідності до чинного законодавства за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів;

2) здійснюється на виконання обов'язку володільця персональних даних, який передбачений законом.

Стаття 21 . Право на виправлення та доповнення персональних даних

1. Суб'єкт персональних даних має право вимагати від особи яка обробляє персональні дані виправлення своїх неточних або недостовірних персональних даних, а також доповнення неповних персональних даних, з урахуванням вимог щодо адекватності, відповідності та ненадмірності відповідно до визначеної мети їх обробки.

2. Особа яка обробляє персональні дані зобов'язана, у строк що не перевищує 30 календарних днів з моменту отримання вимоги:

1) надати суб'єкту персональних даних обгрунтовану відповідь, а у разі наявності підстав - вжити необхідних заходів щодо виправлення або уточнення його персональних даних;

2) повідомити всіх одержувачів персональних даних такого суб'єкта персональних даних, яким були поширені його персональні дані про необхідність виправлення або уточнення таких персональних даних.

3. Одержувачі персональних даних, які отримали повідомлення передбачене частиною третьою цієї статті зобов'язані внести відповідні виправлення або уточнення таких персональних даних у строк що не перевищує 30 календарних днів з моменту отримання повідомлення.

Стаття 22. Право на мобільність персональних даних

1. Суб'єкт персональних даних має право вимагати від володільця персональних даних надання копії масиву будь-яких персональних даних такого суб'єкта, зібраних володільцем персональних даних в процесі автоматизованої обробки у структурованому та машинозчитуваному форматі.

Суб'єкт персональних даних має право на отримання особисто та/або передачу зазначених персональних даних від одного володільця іншому без перешкод з боку першого володільця на підставі відповідного запиту.

2. У тому випадку, якщо реалізація передбаченого частиною першою цієї статті права суб'єкта персональних даних спричиняє додаткові надмірні матеріальні витрати володільця персональних даних та/або пов'язана з надмірними зусиллями, володілець персональних даних має право вимагати компенсації таких витрат за рахунок відповідного суб'єкта персональних даних за умов їх належного обґрунтування. Положення щодо компенсації витрат не застосовується, якщо:

1) внаслідок обробки персональних даних володілець отримав прибуток, розмір якого перевищує витрати на виконання частини першою цієї статті;

2) внаслідок обробки персональних даних було завдано шкоди законним інтересам суб'єкта персональних даних;

3) обробка персональних даних здійснювалася з порушенням вимог цього Закону.

3. Право суб'єкта персональних даних, передбачене цією статтею може бути обмежено виключно на підставі законів України.

4. Реалізація права передбаченого цією статтею не обмежує право суб'єкта персональних даних, передбачене статтею 20 цього Закону.

Стаття 23. Право на заперечення обробки персональних даних

1. Суб'єкт персональних даних має права заперечувати проти обробки його персональних даних, як в цілому так і стосовно окремих категорій його персональних даних або процесів обробки, що застосовуються до таких даних.

2. У разі отримання такого заперечення, особа яка обробляє персональні дані персональних даних повинна припинити обробку, яка заперечується суб'єктом персональних даних, крім випадків, коли підстави такої обробки переважають над правами та інтересами суб'єкта персональних даних, а також випадків, передбачених законом.

3. Якщо персональні дані обробляються з метою прямого маркетингу, суб'єкт персональних даних має право заперечувати проти такої обробки у будь-який час та без будь-яких пояснень чи обґрунтувань. У такому разі отримання заперечення проти обробки персональних даних з метою прямого маркетингу, особа яка обробляє персональні дані:

1) зобов'язана негайно припинити таку обробку та не поновлювати її до отримання відповідної згоди від суб'єкта персональних даних;

2) не має права передавати такі персональних даних іншим особам для їх обробки з метою прямого маркетингу.

Стаття 24. Право на обмеження обробки персональних даних

1 Суб'єкт персональних даних має право вимагати від особи, яка обробляє персональні дані обмежити обробку своїх персональних даних до моменту розгляду вимог про видалення, виправлення, доповнення, передачу персональних даних, а також щодо заперечення їх обробки.

2. Якщо суб'єкт персональних даних заперечує проти обробки своїх персональних даних згідно зі статтею 23 цього Закону, особа яка обробляє такі персональні дані зобов'язана обмежити їх обробку до моменту встановлення того, чи переважають законні інтереси володільця над інтересами або основоположними правами та свободами суб'єкта персональних даних, крім випадків, коли така обробка здійснюється на підставі положень закону.

3. Персональні дані, обробку яких було обмежено на вимогу суб'єкта персональних даних відповідно до положень частин цієї статті, можуть оброблятися лише для зберігання та/або обґрунтування, задоволення, захисту правової вимоги або суспільного інтересу, а також для захисту прав особи чи задоволення суспільного інтересу.

4. В будь-якому випадку про зняття обмежень з обробки персональних даних, накладених на вимогу суб'єкта персональних даних, відповідний суб'єкт повідомляється особою, що здійснює обробку персональних даних до їх зняття.

Стаття 25. Право на захист від автоматизованого прийняття рішень

1. Суб'єкт персональних даних має право оскаржити будь-яке рішення щодо нього прийняте на підставі результатів автоматизованої обробки його персональних даних, в тому числі на підставі результатів автоматизованого профілювання. У разі оскарження таке рішення вважається нечинним з моменту оскарження та підлягає обов'язковому перегляду у неавтоматизованому порядку, за участь людини.

2. Право суб'єкта персональних даних на висловлення своєї думки щодо прийнятого автоматизованого рішення та/або його оскарження є непорушним, а сам процес прийняття такого рішення повинен передбачати можливість людського втручання з боку особи, яка обробляє персональні дані та можливість перегляду прийнятого рішення.

3. Автоматизовані рішення, передбачені положеннями цієї статті, не можуть прийматися на підставі автоматизованої обробки категорій персональних даних, зазначених у статті 6 цього Закону, за винятком випадків надання суб'єктом персональних даних окремої згоди на таку обробку або якщо така обробка здійснюється на виконання вимог, передбачених законами України, за умов забезпечення володільцем персональних даних належного рівня захисту прав, свобод та законних інтересів суб'єктів персональних даних.

Стаття 26. Право знати про обробку персональних даних в цілях прямого маркетингу та заперечувати проти такої обробки

1. Суб'єкт персональних даних має право знати про обробку його персональних даних в цілях прямого маркетингу, у тому числі, з використанням автоматизованих систем телефонних дзвінків, надсилання смс-повідомлень, повідомлень у месенджерах, електронних листів тощо.

2. Обробка персональних даних в цілях прямого маркетингу допускається виключно на підставі згоди суб'єкта персональних даних.

Суб'єкт персональних даних може в будь-який момент відмовитися від обробки його персональних даних на підставі цієї статті, відкликавши свою згоду на таку обробку.

Стаття 27. Право на захист своїх прав та інтересів та відшкодування шкоди

1. Суб'єкт персональних даних має право звертатися із скаргами, пов'язаними з обробкою його персональних даних до Уповноваженого органу або до суду, якщо вважає, що обробка його персональних даних здійснюється з порушенням положень цього Закону.

Право на подання скарги до Уповноваженого органу жодним чином не обмежує право суб'єкта персональних даних на звернення до суду або на захист його прав та інтересів в інший спосіб, передбачений законом.

2. Суб'єкт персональних даних має право на відшкодування матеріальної та/або моральної шкоди, завданої в результаті порушення його прав, передбачених цим Законом за рахунок володільця персональних даних, відповідального за обробку персональних даних відповідного суб'єкта.

Володілець персональних даних звільняється від відповідальності за шкоду, завдану суб'єкту персональних даних, якщо доведе, що події, які спричинили завдання такої шкоди сталися не з його вини.

3. Шкода, завдана суб'єкту персональних даних спільними неправомірними діями/бездіяльністю спільних володільців персональних даних (співволодільців), відшкодовується такими володільцями солідарно, якщо інше не передбачене законом або умовами договору.

Володілець персональних персональних даних, який відшкодував суб'єкту персональних даних шкоду, завдану спільно з іншими володільцями персональних даних, має право вимагати від таких співволодільців відшкодування в порядку регресу пропорційно до їх участі в процесах обробки персональних даних, якими було завдано шкоду.

Стаття 28. Реалізація прав суб'єкта персональних даних та форма комунікації

1. Вимоги суб'єкта персональних, пов'язані з реалізацією ним своїх прав, передбачених цим Законом, надаються особам, які обробляють персональні дані особисто або через представника, у тому числі з використанням засобів зв'язку та телекомунікаційних сервісів, в усній, письмовій чи електронній формі.

Незалежно від обраної форми звернення, суб'єкт персональних даних зобов'язаний вжити всіх необхідних заходів для його ідентифікації особою яка обробляє персональні дані, в якості автора вимоги, а також забезпечити належне підтвердження своєї особи та повноважень осіб, що його представляють.

2. Особа, яка обробляє персональні дані, зобов'язана розглянути кожну вимогу суб'єкта персональних даних та виконати таку вимогу, у випадку її обґрунтованості.

3. Про кожне рішення, що стосується розгляду вимог, а також будь-яких інших звернень суб'єкта персональних даних, пов'язаних з реалізацією передбачених цим Законом прав, особа яка обробляє персональні дані повідомляє відповідного суб'єкта в строк, що не перевищує 30 календарних днів, якщо інше не встановлено цим Законом.

4. Реалізація прав суб'єкта персональних даних, передбачених положеннями цього Закону, не повинна порушувати права та свободи інших осіб та/або порушувати вимоги законодавства.

Володілець персональних даних зобов'язаний вжити всіх можливих законних заходів для уникнення порушення прав і свобод людини або мінімізації ризиків їх порушення.

5. Задоволення вимог, а також будь-яких інших звернень, пов'язаних з реалізацією передбачених цим Законом прав, поданих/надісланих суб'єктом персональних даних з обмеженою (неповною) дієздатністю особисто, підлягають задоволенню в межах правовідносин, учасниками яких зазначені особи можуть вступати особисто згідно із законом без згоди батьків/усиновлювачів, опікунів/піклувальників.

Розділ IV
СУБ'ЄКТИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЇХНІ ОБОВ'ЯЗКИ

Стаття 29 Суб'єкти обробки персональних даних

До суб'єктів обробки персональних даних відносяться:

володілець персональних даних;

співволодільці персональних даних;

розпорядник персональних даних.

Стаття 30. Обов'язки володільця персональних даних

1. Обов'язки володільця персональних даних:

1) вживати всі можливі правові, організаційні, технічні та інші заходи з метою забезпечення дотримання вимог законодавства про захист персональних даних з урахуванням цілей, обсягу, специфіки, обробки персональних даних, а також пов'язаних з такою обробкою ризиків порушення прав суб'єктів персональних даних, забезпечувати перегляд та актуалізацію відповідних заходів;

2) обробляти персональні дані лише з тією метою, з якою вони були зібрані на підставі згоди суб'єкта персональних даних або інших законних підставах ;

3) повідомити всіх осіб, яким були поширені персональні дані, про обмеження щодо їх обробки, накладених за запитом суб'єкта персональних даних, відповідно до статей ____ цього Закону, за винятком випадків, коли таке повідомлення є неможливим;

4) надавати за запитом суб'єкта персональних даних інформацію про всіх осіб, яким були поширені його персональні дані, крім випадків, передбачених законами України;

5) нанести спеціальні позначки (текстові або графічні знаки), які ідентифікують володільця персональних даних на копії (скан-копії, фотокопії тощо) документів, що містять персональні дані, перед їх оприлюдненням/поширенням, зокрема, у мережі Інтернет;

6) наносити спеціальні позначки (текстові або графічні знаки) володільця або розпорядника персональних даних на копіях (скан-копіях, фотокопіях тощо) офіційних документів, що містять персональні дані (документах, що посвідчують особу, довідках про присвоєння ідентифікаційного номера, свідоцтвах про державну реєстрацію актів цивільного стану, військових квитках, посвідченнях, перепустках тощо) під час їх збирання у суб'єкта персональних даних (до початку їх фактичного зберігання);

7) видалити або знеособити персональні дані, якщо їх обробка більше не потрібна для досягнення визначеної мети або мета досягнута, без додаткових вимог щодо видалення або знеособлення персональних даних від суб'єктів, чиї персональні дані обробляються;

8) повідомити суб'єкта про обробку/можливість обробки його персональних даних для цілей прямого маркетингу одночасно із збором/отриманням таких даних та забезпечити відповідному суб'єкту можливість відмовитися від такої обробки та негайно її припинити у разі отримання відповідної відмови;

9) повідомити суб'єкта про обробку його персональних даних спільно з іншими володільцями персональних даних (у випадку наявності), а також про залучення до обробки його персональних даних розпорядників, їх кількість, ідентифікаційні, контактні дані та обсяг делегованих їм прав;

10) чітко визначити обсяг прав та обов'язків розпорядників персональних даних шляхом укладення відповідних угод (договорів), якщо інше не передбачено нормами чинного законодавства;

11) повідомити суб'єкта персональних даних про обробку його персональних даних, що передбачає здійснення/можливість здійснення передачі за межі державного кордону України (транскордонної передачі), у тому числі мету такої передачі, суб'єктів, яким персональні дані передаються, способи їх передачі;

12) повідомляти Уповноважений орган про процеси обробки персональних даних та зміни в таких процесах у випадках, передбачених цим Законом в порядку, визначеному Уповноваженим органом;

13) довести правомірність відмови у виконанні вимог суб'єкта персональних даних щодо обмежень обробки або її припинення, видалення, зміни, відновлення, доступі до персональних даних;

14) виконувати законні вимоги Уповноваженого органу;

15) відшкодувати шкоду, заподіяну суб'єкту персональних даних внаслідок неправомірної обробки його персональних даних та/або порушенням вимог законодавства в сфері захисту персональних даних;

16) бути здатним довести, що ним виконано всі вимоги цього Закону;

17) виконувати інші обов'язки, які виникають в процесі реалізації положень цього Закону.

2. Володілець персональних даних несе повну відповідальність за порушення прав суб'єкта персональних даних, а також встановлених законодавством вимог в сфері захисту персональних даних, якщо інше не передбачено законом;

3. Володілець персональних даних, який відшкодував суб'єкту персональних даних шкоду, завдану діями розпорядника персональних даних, має право вимагати від такого розпорядника відшкодування в порядку регресу, якщо заподіяння шкоди відбулось не з вини відповідного володільця персональних даних.

Стаття 31. Спільні володільці (співволодільці) персональних даних

1. Володільці персональних даних, які спільно визначають цілі обробки персональних даних одного й того ж суб'єкта/кола суб'єктів та обробляють такі персональні дані, вважаються спільними володільцями (співволодільцями) персональних даних.

2. Обсяг відповідальності, а також інші питання взаємодії між співволодільцями персональних даних в процесі здійснення обробки таких даних визначаються відповідними угодами (договорами), якщо інше не передбачено законом.

Відсутність укладених угод/інших документів не позбавляє осіб, що здійснюють обробку персональних даних у спосіб, передбачений частиною першою цієї статті, статусу співволодільців персональних даних та не звужує коло їхніх обов'язків відносно суб'єкта персональних даних.

3. Співволоділець персональних даних, на запит суб'єкта персональних даних, зобов'язаний надати останньому можливість ознайомитися з усіма положеннями укладених між співволодільцями угод, які стосуються обробки персональних даних, реалізації прав суб'єкта персональних даних та ідентифікуючих і контактних даних сторін. Така можливість ознайомитися, на вимогу суб'єкта персональних даних, може бути реалізована у вигляді надання витягу із договору, який містить відповідні положення.

4. Частина третя цієї статті не застосовуються якщо обсяг відповідальності, а також інші питання взаємодії між співволодільцями персональних даних визначено положеннями нормативно-правових актів

5. Незалежно від наявності/відсутності визначення між співволодільцями персональних даних конкретного обсягу відповідальності, пов'язаної зі спільною обробкою персональних даних, суб'єкт персональних даних може реалізовувати свої права, передбачені цим Законом, по відношенню до будь-якого спільного володільця в повному обсязі.

6. За обсягом обов'язків по відношенню до конкретного суб'єкта персональних даних співволоділець та володілець персональних даних є тотожними суб'єктами в контексті обробки персональних даних.

Стаття 32. Розпорядник персональних даних

1. Розпорядник персональних даних може залучатися до обробки персональних даних на підставі угоди (договору), укладеного з володільцем персональних даних або на підставі положень нормативно-правових актів.

3. Обсяг пов'язаних з обробкою персональних даних прав, переданих розпоряднику персональних даних володільцем не може бути ширшим ніж той, що був отриманий володільцем персональних даних від суб'єкта персональних даних та/або встановлений положеннями нормативно-правових актів.

4. Поширення розпорядником персональних даних отриманих від володільця персональних даних прав на обробку персональних даних, а також залучення до виконання укладених з володільцем персональних даних інших розпорядників, можливе лише за умов, якщо таке право розпорядника персональних даних прямо передбачено умовами укладених з володільцем персональних даних угод (договорів, регламентів тощо) або положеннями нормативно-правових актів.

Про факт залучення до обробки персональних даних інших розпорядників розпорядник персональних даних повідомляє володільця таких даних невідкладно, але не пізніше, ніш в строк, що не перевищує 3 робочі дні з дня залучення.

5. Розпорядник персональних даних не може самостійно визначати цілі обробки персональних даних, які він отримав та обробляє як розпорядник. В разі визначення самостійно цілей обробки персональних даних щодо персональних даних, які розпорядником отримані від володільця персональних даних, такий розпорядник вважається володільцем персональних даних, що обробляються ним із власною метою та зобов'язаний дотримуватись усіх вимог, встановлених цим Законом до володільця персональних даних.

6. Розпорядник персональних даних несе відповідальність перед володільцем персональних даних за порушення прав суб'єктів персональних даних в обсязі, визначеному на підставі угоди (договору) з володільцем персональних даних, якщо інше не визначено законом.

Розпорядник персональних даних звільняється від відповідальності за дії з персональними даними, що призвели до порушення прав суб'єктів персональних даних та/або вимог законодавства в сфері захисту персональних даних, якщо такі дії були вчинені на підставі прямих вказівок (доручень) володільця персональних даних та/або угод (їх окремих положень тощо), укладених з володільцем персональних даних, за винятком випадків, якщо такі вказівки/угоди були завідомо та очевидно неправомірними/злочинними.

7. Угоди (договори), предметом яких є обробка персональних даних, укладаються між володільцем та розпорядником персональних даних в письмовій (прирівняній до письмової) формі, повинні містити обов'язкові умови, які визначають мету, вид, способи та строки обробки персональних даних, категорії суб'єктів, чиї персональні дані обробляються, а також обсяг прав і обов'язків сторін в частині обробки відповідних персональних даних.

Обсяг прав розпорядника персональних даних щодо обробки персональних даних не може бути ширшим, ніж обсяг прав та обов'язків володільця персональних даних, у тому числі, в тих

випадках, коли правовідносини між володільцем та розпорядником персональних даних врегульовані положеннями нормативно-правових актів.

8. Після припинення правовідносин між володільцем та розпорядником персональних даних, обробка всіх персональних даних, поширених/переданих розпоряднику персональних даних або зібраних ним в інтересах володільця персональних даних припиняється, а відповідні персональні дані знищуються або повертаються володільцю персональних даних з їх подальшим знищенням розпорядником персональних даних, крім випадків, коли чинне законодавство вимагає вчинення інших дій.

9. Розпорядник персональних даних на вимогу володільця персональних даних зобов'язаний підтвердити вжиття всіх необхідних заходів щодо організації належного рівня захисту персональних даних при їх обробці відповідно до вимог законодавства та укладених з володільцем персональних даних угод.

У випадку неспроможності підтвердити вжиття зазначених заходів, володілець персональних даних зобов'язаний вимагати припинення (призупинення в окремій частині) обробки персональних даних їх розпорядником до моменту усунення всіх недоліків в обробці персональних даних та вжиття заходів щодо їх захисту в повному обсязі.

Невжиття розпорядником заходів щодо організації належного рівня захисту персональних даних при їх обробці є підставою для припинення правовідносин між ним та володільцем персональних даних шляхом розірвання укладених угод (договорів, регламентів тощо).

10. Розпорядник персональних даних зобов'язаний утриматись від виконання явно неправомірних/злочинних вказівок/доручень володільця персональних даних, а також умов угод (договорів, регламентів тощо), що явно призводять/можуть призвести до порушення прав суб'єктів персональних даних та/або вимог законодавства в сфері захисту персональних даних.

11. Про будь-які виявлені дії володільця персональних даних, що призводять/можуть призвести до порушення прав суб'єкта персональних даних та/або вимог законодавства в сфері захисту персональних даних, розпорядник персональних даних зобов'язаний повідомити відповідного володільця персональних даних невідкладно, але не пізніше, ніш в строк, що не перевищує 3 робочі дні з дня виявлення таких дій.

Стаття 33. Загальні вимоги до безпеки обробки персональних даних

1. До загальних (обов'язкових) організаційних, технічних та інших заходів, які зобов'язані вживати суб'єкти, що здійснюють обробку персональних даних для захисту персональних даних в процесі їх обробки належать:

1) Обов'язкове відібрання від працівників та інших осіб, які мають/можуть мати доступ до персональних даних в процесі виконання своїх посадових (трудових) обов'язків зобов'язань про нерозголошення персональних даних, які стали їм відомі в процесі обробки.

Відповідні зобов'язання відбираються до моменту залучення працівників до обробки персональних даних/до моменту отримання доступу до таких даних іншими особами.

2) Розмежування рівня доступу до персональних даних працівниками/іншими особами на яких володільцем покладено обов'язок щодо обробки персональних даних (зокрема на підставі цивільно-правових угод), у тому числі за допомогою апаратно-програмних засобів контролю за доступом до приміщень, в яких здійснюється обробка персональних даних, використання персональних логінів/паролів (інших засобів ідентифікації/верифікації) при роботі з інформаційними, інформаційно-телекомунікаційними системами тощо.

3) Забезпечення загальної безпеки персональних даних, у тому числі, їх захисту від втрати, пошкодження, знищення, викрадення тощо, зокрема шляхом обладнання приміщень, в яких здійснюється обробка персональних даних засобами блокування несанкціонованого доступу (в

залежності від ступеня ризику несанкціонованого доступу) - надійними вхідними дверима, гратами/ролетами на вікнах, сигналізацією, охороною , засобами протипожежної охорони тощо.

В інформаційних, інформаційно-телекомунікаційних системах, відповідні заходи забезпечуються шляхом встановлення на обладнанні, за допомогою якого здійснюється обробка персональних даних, захисного програмного забезпечення від вірусних, шпигунських та інших шкідливих програм.

У випадках, передбачених законодавством, вимоги щодо захисту інформації в інформаційних, інформаційно-телекомунікаційних визначається окремими нормативно-правовими актами.

4) Забезпечення максимально оперативного та повного відновлення втрачених/пошкоджених або знищених персональних даних персональних, зокрема шляхом створення надійно захищених резервних копій таких даних (їхніх масивів).

5) Забезпечення належних професійних якостей у осіб, відповідальних за обробку персональних даних, зокрема шляхом організації, у випадку необхідності, їхнього навчання, підвищення кваліфікації, сертифікації тощо.

2. Суб'єкт, який здійснює обробку персональних даних звільняється від відповідальності, якщо ним були вжиті всі необхідні заходи щодо безпеки персональних даних, а несанкціонований доступ до таких даних відбувся внаслідок злочинних або неправомірних дій третіх осіб.

Стаття 34. Повідомлення про порушення безпеки (режиму захисту) персональних даних

1. У разі порушення безпеки персональних даних внаслідок витоку, несанкціонованого доступу або порушення їх цілісності володілець персональних даних зобов'язаний повідомити про це:

суб'єкта, стосовно персональних якого відбулося порушення режиму безпеки;

співволодільців персональних даних;

розпорядників персональних даних;

Уповноважений орган - в порядку, визначеному Уповноваженим органом.

2. Повідомлення повинно містити опис подій, внаслідок яких відбулося порушення безпеки персональних даних (витік, несанкціонований доступ, порушення цілісності), відомі причини порушення безпеки та про вжиті заходи щодо відновлення безпеки персональних даних та/або про неможливість її відновлення (в цілому чи окремій частині) із зазначенням причин.

3. Розпорядник персональних даних про факт порушення безпеки персональних даних одночасно повідомляє суб'єкта персональних даних та володільця персональних даних з урахуванням вимог до повідомлення, передбачених частиною 2 цієї статті.

4. Передбачені цією статтею повідомлення здійснюються невідкладно, але не пізніше ніж протягом 72 годин від моменту, коли відповідний суб'єкт обробки персональних даних дізнався/міг дізнатися про порушення безпеки персональних даних що ним обробляються.

5. Повідомлення державних органів, а також юридичних осіб публічного права, діяльність яких регламентована положеннями нормативно-правових актів можуть здійснюватися шляхом розміщення публічних оголошень в офіційних виданнях, на офіційних веб-сторінках чи за допомогою державних інформаційно-телекомунікаційних ресурсів за умов, якщо місце та порядок розміщення повідомлення затверджене в офіційно оприлюдненому нормативно-правовому акті.

Стаття 35. Оцінка ризиків порушення прав суб'єкта, пов'язаних з обробкою його персональних даних

1. Ступінь ризику порушення прав суб'єкта, пов'язаний з обробкою його персональних даних (далі - ступінь ризику), підлягає оцінці володільцем персональних даних до початку здійснення обробки таких даних.

2. Комплекс заходів, запровадження яких є необхідним для забезпечення належного захисту прав суб'єкта персональних даних, визначається володільцем персональних даних з урахуванням результатів здійсненої оцінки ступеня ризику.

3. Оцінка ступеня ризику здійснюється з урахуванням критеріїв ризику та в порядку, які затверджуються Уповноваженим органом.

Стаття 36. Особа, відповідальна за захист персональних даних

1. Володілець та розпорядник персональних даних може призначити особу, відповідальну за обробку та захист персональних даних (далі - відповідальна особа), на яку покладаються функції з організації правового, технічного та методологічного забезпечення процесів обробки персональних даних.

2. У випадку покладення функції з організації правового, технічного та методологічного забезпечення процесів обробки персональних даних на структурний підрозділ володільця або розпорядника персональних даних, відповідальною особою вважатиметься керівник відповідного структурного підрозділу.

3. Призначення відповідальної особи є обов'язковим, якщо:

особа, що здійснює обробку персональних даних є державним органом, органом місцевого самоврядування;

державним або комунальним підприємством, установою, організацією, закладом що належать до сфери управління державного органу або органу місцевого самоврядування;

володільцем та розпорядником персональних даних здійснюється обробка персональних даних (разом або кожним окремо) 100 і більше (?)[1] суб'єктів персональних даних;

володільцем та розпорядником персональних даних здійснюється обробка персональних даних (разом або кожним окремо), передбачених частиною першою статті 7 цього Закону, які належать 50 і більше (?) суб'єктам персональних даних.

4. У разі якщо кількість суб'єктів персональних даних чиї дані обробляються володільцем або розпорядником в десять чи більше разів перевищує кількість визначену частиною третьою цієї статті Закону - особа, відповідальна за захист персональних даних призначається як окрема посада, до посадових обов'язків якої може входити виключно організація роботи пов'язаної з обробкою та захистом персональних даних або визначається (створюється) окремий структурний підрозділ відповідальний за захист персональних даних.

5. Особа, відповідальна за захист персональних даних може бути призначена з числа працівників володільця або розпорядника, за умови що такий працівник, з огляду на свої посадові повноваження може впливати на усі процеси обробки персональних даних володільця або розпорядника, а його рішення щодо обробки персональних даних є обов'язковими для виконання іншими працівниками володільця або розпорядника персональних даних.

6. Вимоги до кваліфікації та професійних знань особи, відповідальної за захист персональних даних, керівника та працівників окремого структурного підрозділу відповідального за захист персональних даних встановлюються Уповноваженим органом.

---

[1] Підлягає обговоренню

7. Уповноваженим органом затверджуються типова посадова інструкція особи, відповідальної за захист персональних даних та типове положення про структурний підрозділ відповідальним за захист персональних даних.

Стаття 37 Загальні функції та обов'язки відповідальної особи або структурного підрозділу відповідального за захист персональних даних

1. Під час забезпечення захисту персональних даних в процесі їх обробки на відповідальна особа або структурний підрозділ:

організовує правове, технічного та методологічного забезпечення процесів обробки персональних даних, проводить їх моніторинг та аудит;

організовує облік операцій, пов'язаних із доступом до персональних даних;

інформує володільця/розпорядника персональних даних (його керівника) про необхідність вжиття заходів щодо захисту персональних даних, якщо їх вжиття потребує їх безпосередню участь;

відбирає від працівників та інших осіб, які мають/можуть мати доступ до персональних даних в процесі виконання своїх посадових (трудових) обов'язків зобов'язань про нерозголошення персональних даних, які стали їм відомі в процесі обробки;

організовує взаємодію з суб'єктами персональних даних, у тому числі забезпечує задоволення законних вимог відповідних суб'єктів;

організовує, з урахуванням вимог закону, доступ до персональних даних третіх осіб;

організовує оцінку та моніторинг ризиків порушення прав суб'єкта, пов'язаних з обробкою його персональних даних;

забезпечує взаємодію з Уповноваженим органом.

Розділ V

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 38. Правопорушення у сфері захисту персональних даних

1. Вчинення правопорушень у сфері захисту персональних даних тягне за собою відповідальність, передбачену цим Законом та іншими законами України.

Стаття 39. Відповідальність за порушення законодавства в сфері захисту персональних даних

1. Рішення про притягнення до відповідальності осіб за вчинені ними правопорушення в сфері захисту персональних даних, а також про застосування інших заходів, приймається Уповноваженим органом в порядку, визначеному законодавством.

2. До відповідальності передбаченої статтею 40 цього Закону можуть бути притягнені лише володільці або розпорядники персональних даних.

3. У випадку призначення володільцем або розпорядником персональних даних відповідальної особи, адміністративна відповідальність за порушення законодавства в сфері захисту персональних даних покладається на таку особу.

Відповідальна особа звільняється від адміністративної відповідальності, якщо нею були вжиті усі передбачені законом заходи щодо захисту персональних даних або про необхідність їх вжиття був своєчасно повідомлений керівник володільця/розпорядника персональних даних, якщо для вжиття відповідних заходів вимагається безпосередня участь керівника.

Якщо володілець або розпорядник персональних даних є юридичною особою, відповідальність за порушення законодавства в сфері захисту персональних даних, за відсутності призначеної відповідальної особи, покладається на керівника відповідної юридичної особи.

4. Притягнення винних осіб до фінансової, адміністративної або кримінальної відповідальності не позбавляє суб'єктів персональних даних, чиї права були порушені, звернутися за компенсацією в порядку передбаченому цивільним законодавством.

Стаття 40. Відповідальність володільців та розпорядників за порушення законодавства у сфері захисту персональних даних[2]

1. Порушення вимог передбачених статтями 12 - 14 цього Закону, що призвело до порушення прав суб'єктів персональних даних -

тягне за собою накладення штрафу у розмірі від п'ятисот неоподатковуваних мінімумів доходів громадян до 0,085 відсотків загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф, в залежності від того що вище, за кожне окреме порушення вимог Закону, що призвело до порушення прав кожного окремого громадянина.

2. Порушення вимог передбачених статтями статтями 3, 8, 9, 11, 15, 17, 18, 19 - 26; частинами першою – третьою, п'ятою – дев'ятою, одинадцятою статті 30 цього Закону, що призвело до порушення прав суб'єктів персональних даних -

тягне за собою накладення штрафу у розмірі від однієї тисячі неоподатковуваних мінімумів доходів громадян до 0,17 відсотків загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф, в залежності від того що вище, за кожне окреме порушення вимог Закону, що призвело до порушення прав кожного окремого громадянина;

3. Порушення вимог передбачених статтею 7 цього Закону, що призвело до порушення прав суб'єктів персональних даних -

тягне за собою накладення штрафу у розмірі від двох тисяч неоподатковуваних мінімумів доходів громадян до 0,34 відсотків загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф, в залежності від того що вище, за кожне окреме порушення вимог Закону, що призвело до порушення прав кожного окремого громадянина;

4. Невиконання законних вимог та приписів Уповноваженого органу -

---

[2] Розміри штрафів наведені орієнтовно

тягне за собою накладення штрафу у розмірі від однієї тисячі неоподатковуваних мінімумів доходів громадян до 0,17 відсотків загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф, в залежності від того що вище.

5. Невиконання законних вимог та приписів Уповноваженого органу, якщо такі вимоги полягають у припиненні порушення прав суб'єктів персональних даних або поновленні порушених прав суб'єктів персональних даних -

тягне за собою накладення штрафу у розмірі від п'ятисот неоподатковуваних мінімумів доходів громадян до 0,085 відсотків загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф, в залежності від того що вище, за порушення прав кожного окремого суб'єкта персональних даних.

6. Відсутність передбачених законом документів, розробка та затвердження яких є обов'язковою для суб'єктів, що здійснюють обробку персональних даних -

тягне за собою збільшення розміру штрафу передбаченого частинами першою - третьою цієї статті Закону на тридцять відсотків.

7. Кожне повторне порушення вимог Закону вчинене упродовж року тягне за собою накладення штрафу у розмірі двохсот відсотків від розміру раніше накладеного штрафу.

8. Якщо в межах однієї і тієї ж обробки персональних даних або кількох пов'язаних між собою операцій обробки персональних даних володілець або розпорядник персональних даних допустив порушення декількох вимог передбачених статтями цього Закону сукупний розмір штрафу не повинен перевищувати розмір штрафу за найбільш серйозне порушення. Зазначене положення не поширюється на випадки передбачені частинами шостою та сьомою цієї статті Закону.

9. Загальні розміри штрафів, передбачених частинами першою - третьою цієї статті Закону не можуть перевищувати такі межі:

для штрафів передбачених частиною першою цієї статті Закону максимальний розмір штрафу становить півтора відсотки загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф;

для штрафів передбачених частиною другою цієї статті Закону максимальний розмір штрафу становить два відсотки загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф;

для штрафів передбачених частиною першою цієї статті Закону максимальний розмір штрафу становить чотири відсотки загального річного обороту суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф.

Стаття 41. Строки давності для застосування фінансової відповідальності

1. Суб'єкт господарювання не може бути притягнений до фінансової відповідальності за порушення законодавства про захист персональних даних, якщо минув строк давності притягнення до відповідальності.

Строк давності притягнення до фінансової відповідальності за порушення законодавства про захист персональних даних становить три роки з дня вчинення порушення, а в разі триваючого порушення - з дня закінчення вчинення порушення.

2. Перебіг строку давності зупиняється на час розгляду Уповноваженим органом справи про порушення законодавства в сфері захисту персональних даних, а також на час розгляду відповідної справи у суді.

Розділ ___

Прикінцеві та перехідні положення

Список представників Секретаріату Уповноваженого для включення в робочу групу

1. **Берназюк Інна Миколаївна**, представник Уповноваженого у сфері захисту персональних даних;
2. **Барвіцький Віктор Юрійович**, представник Уповноваженого з дотримання права на інформацію та представництва в Конституційному Суді України;
3. **Ніколаєв Андрій Вікторович**, директор Департаменту у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини;
4. **Щербина Наталія Леонідівна**, заступник директора Департаменту – начальник відділу нормативно-правового забезпечення Департаменту у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини.