

Як суб'єкт персональних даних може захистити свої права у період воєнного стану?

Для громадянина

Важливою умовою правомірної обробки персональних даних у період дії правового режиму воєнного стану є забезпечення громадянам належного рівня захисту їхніх прав, пов'язаних з персональними даними.

Відповідно до ч. 1 ст. 8 Закону України «Про захист персональних даних», особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

Основний перелік цих прав закріплений у ч. 2 ст. 8 вказаного Закону України.

У вирішенні питання про можливість ефективного захисту прав громадян як суб'єктів персональних даних необхідно виходити з правового та технологічного аспектів цього питання.

Сутність правового аспекту виявляється у визначенні кола прав суб'єктів персональних даних, оптимального механізму і суб'єктів такого захисту.

Технологічний аспект виявляється у необхідності дотримання певних рекомендацій, спрямованих на безпечну обробку інформації про фізичну особу за допомогою інформаційно-телекомунікаційних технологій і систем, а також вчинення суб'єктами персональних даних окремих дій чи відмови від їх вчинення.

Відповідно до п. 7 ч. 2 ст. 8 Закону України «Про захист персональних даних», кожна фізична особа має право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи.

Реалізація зазначеного права допускається як через застосування правових засобів захисту шляхом самозахисту, так, і через направлення скарг до Уповноваженого Верховної Ради України з прав людини, або звернення з позовом до суду про захист своїх прав як суб'єкта персональних даних.

Серед способів самозахисту прав, якими згідно з чинним законодавством можуть скористатися суб'єкти персональних даних слід вказати на наступні:

- Направляти запити щодо одержання інформації про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом.
- отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, безкоштовну відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних. Необхідно звернути увагу, суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання інформації, визначеної у пункті 1 частини четвертої цієї статті, крім випадків, установлених законом.
- висувати вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних.
- висувати вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними.
- відкликати згоду на обробку персональних даних (у випадку, якщо таку згоду було надано).

Кожен із зазначених способів самозахисту прав суб'єктів персональних даних може реалізуватися самостійно носієм цих прав або уповноваженою нею особою без додаткових звернень до Уповноваженого Верховної Ради України з прав людини, суду чи правоохоронних органів.

Самозахист прав суб'єктом персональних даних також не виключає можливість його звернення до уповноважених органів за захистом порушених прав чи законних інтересів, у відносинах, пов'язаних з обробкою персональних даних.

Згідно з п., п. 1 та 2 ч. 1 ст. 22 Закону України «Про захист персональних даних», контроль за додержанням вимог законодавства про захист персональних даних в Україні покладається на Уповноваженого Верховної Ради України та суд.

Перший з вказаних суб'єктів владних повноважень здійснює заходи з поновлення прав суб'єктів персональних даних як з власної ініціативи (у разі виявлення фактів порушення законодавства про захист персональних даних при проведенні моніторингу стану додержання прав і свобод людини, здійснення планових або позапланових перевірок у відповідній сфері правового регулювання), так, і з ініціативи потерпілих осіб.

В останньому випадку підставою для застосування засобів правового захисту прав суб'єктів персональних даних є скарга потерпілої особи, або її уповноваженого представника, направлена на адресу Уповноваженого Верховної Ради України.

Звертаємо увагу, скарги про порушення прав суб'єктів персональних даних подаються до Уповноваженого Верховної Ради України з прав людини з обов'язковим додержанням вимог, передбачених у ст. 5 Закону України «Про звернення громадян».

На підставі п. 5 ч. 1 ст. 23 Закону України «Про захист персональних даних», за підсумками перевірки, розгляду звернення, Уповноважений Верховної Ради України має право видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних.

Такі приписи направляються порушнику у письмовій формі і є обов'язковими до виконання.

У випадку, якщо в діях посадових осіб володільців/розпорядників персональних даних при проведенні перевірки виявлені ознаки порушень, передбачених ст. 188-39, 188-40 Кодексу України про адміністративні правопорушення, уповноважені посадові особи Уповноваженого Верховної Ради України з прав людини мають право складати протоколи про адміністративні правопорушення та направляти їх до суду з метою притягнення винних осіб до адміністративної відповідальності.

Звертаємо увагу, кожна особа, чиї права як суб'єкта персональних даних були порушені може безпосередньо звернутися з позовом до суду про їх захист чи поновлення.

Зважаючи на характер порушення, суд може застосувати для поновлення прав суб'єктів персональних даних, передбачений у ст. 5 Цивільного процесуального кодексу України та ст. 5 Кодексу адміністративного судочинства.

Що ж до технологічного аспекту захисту прав суб'єктів персональних даних, то основні рекомендації, які ним охоплюються можна звести до наступних:

- Слід уникати відвідування сайтів або використання цифрових застосунків, у безпечному використанні яких ви не впевнені повністю.
- Слід за можливістю при авторизації в інформаційних системах, сайтах, електронних кабінетах використовувати дво або багатофакторну аутентифікацію.
- Перед початком завантаження та/або роботи із сайтами, мобільними застосунками, іншими інформаційними ресурсами необхідно ознайомитися з політикою конфіденційності, іншими правилами обробки персональних даних, розробленими володільцями таких ресурсів.
- Не надавати свої персональні дані та згоду на їх обробку, до моменту ознайомлення суб'єкта персональних даних з метою та підставами обробки персональних даних, а також умовами їх обробки з боку володільця, крім випадків, коли відповідна обробка здійснюється на підставі дозволу, наданого законом, для виконання володільцем покладених на нього обов'язків.
- Обмеження використання інформаційних ресурсів, сайтів, мобільних застосунків, лише перевіреними та такими, що необхідні суб'єкті персональних даних.
- У разі неповідомлення володільцем персональних даних про видалення або знищення персональних даних після спливу мети їх обробки направлення

вимоги про вчинення відповідних дій та зобов'язання припинити їх подальшу обробку.

- Відмову від передачі персональних даних, включаючи паролі доступу до акаунтів, разові паролі, дані геолокації, тощо третім особам до моменту виникнення законних та необхідних підстав для збору такої інформації.

При вирішенні питання щодо можливості застосування тих або інших інструментів захисту прав суб'єктів персональних даних необхідно враховувати, чи має місце порушення або правомірне обмеження таких прав.

Відповідно до п. 3 Указу Президента України від 24.02.2022 року № 64/2022 «Про запровадження воєнного стану в Україні», затвердженого Законом України від 24.02.2022 року № 2102-IX, у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені ст. 30 - 34, 38, 39, 41 - 44, 53 Конституції України. забезпечення Зі змісту вказаного Указу Президента України слідує можливість встановлення в нормах законів України тимчасових обмежень права на невтручання в особисте і сімейне життя, включаючи прав, пов'язаних з обробкою персональних даних.

Відповідно до ч. 1 ст. 32 Конституції України, ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

Як слідує з буквального змісту наведеної норми, перелік підстав для втручання в особисте сімейне життя, зокрема, шляхом збирання і обробки інформації про фізичну особу є імперативним і визначається виключно Конституцією України.

Згідно з приписами ч. 2 ст. 32 Конституції України не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Вказана конституційна норма спирається на стандарти Ради Європи, закладені у ст. 8 Конвенції Ради Європи «Про захист прав людини і основоположних свобод».

Згідно з вказаними положеннями Конвенції, кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції.

Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Отже, ч. 2 ст. 32 Конституції України та ч. 2 ст. 8 Конвенції Ради Європи «Про захист прав людини та основоположних свобод» визначено, вичерпний перелік підстав для обробки персональних даних без згоди суб'єкта персональних даних та обмеження їхніх прав в нормах національного законодавства України.

Прояв у конкретних відносинах одного чи декількох з вказаних випадків означає відсутність ознак порушення прав суб'єктів персональних даних, а від так допускає можливість захисту суб'єктами персональних даних своїх прав лише в частині, що не охоплюється дією вище вказаних норм.

Для суб'єктів владних повноважень.

При вирішенні питання щодо захисту персональних даних, чинне законодавство у відношенні до суб'єктів владних повноважень закріпило правило, відповідно до якого, у випадку покладення на конкретного з цих суб'єктів функцій володільця, на нього також одночасно покладаються завдання по забезпеченню належного захисту персональних даних, які перебувають у його володінні.

Відповідно до ч. 1 ст. 24 Закону України «Про захист персональних даних», володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Володільць, розпорядник персональних даних вживають заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

При цьому, володільць, розпорядник персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з

урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки, п. п. 3.1. та 3.2. п. 3 «Типового порядку обробки персональних даних», затвердженого наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 року № 1/08-14..

Фактично, вказані положення «Типового порядку обробки персональних даних» встановлюють правила, відповідно до яких, способи правового, організаційного та технічного захисту персональних даних повинні визначатися в актах національного законодавства з урахуванням особливостей обробки, правового режиму персональних даних, статусу інформаційно-телекомунікаційної системи, публічного реєстру, де буде проводитися опрацювання персональних даних.

Згідно з положеннями ст. 11 Конвенції «Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, кожна Сторона зобов'язується встановити відповідні санкції та засоби правового захисту стосовно порушень положень внутрішнього права, що запроваджують основоположні принципи захисту персональних даних, визначені у главі другій цієї Конвенції.

З наведеної норми слідує, що зобов'язання держав-членів Конвенції щодо забезпечення належного захисту персональних даних охоплюють всі дії, пов'язані з обробкою персональних даних.

В цьому аспекті, для суб'єктів владних повноважень важливо визначити у власних підзаконних актах або на рівні постанов Кабінету Міністрів України спеціальний порядок захисту персональних даних, відповідний функціям публічних реєстрів, інформаційно-телекомунікаційних систем, а також визначити методи такого правового захисту.

Відповідно до п. 3.4. п. 3 «Типового порядку обробки персональних даних», організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників володільця/розпорядника;
- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярне навчання співробітників, які працюють з персональними даними.

Щодо технічних заходів, їх система формулюється на початковому етапі проектування інформаційно-телекомунікаційної системи, реєстру у технічному завданні на створення/модернізацію такого об'єкта.

На наступному етапі – введення інформаційної системи або реєстру в експлуатацію важливо визначити види технічних заходів, які будуть застосовуватися для захисту персональних даних у правовстановлюючому акті для такої системи/реєстру.

Як зазначено у п. 3.5. п. 3 «Типового порядку обробки персональних даних», володільць/розпорядник веде облік працівників, які мають доступ до персональних даних суб'єктів. Володільць/розпорядник визначає рівень доступу зазначених працівників до персональних даних суб'єктів. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків.

Усі інші працівники володільця/розпорядника мають право на повну інформацію лише стосовно власних персональних даних.

При цьому, працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

Датою надання права доступу до персональних даних вважається дата надання зобов'язання відповідним працівником, підпункти 3.5. – 3.8. пункту 3 «Типового порядку обробки персональних даних».

Для забезпечення належного правового захисту персональних даних, володільцем яких виступає суб'єкт владних повноважень, при проектуванні публічних реєстрів та/або інформаційних систем важливо здійснити автоматизованих розподіл доступу працівників до файлів персональних даних за принципом рольового поділу користувачів відповідних інформаційних об'єктів.

У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику.

Таким чином, діяльність суб'єктів владних повноважень у період існування режиму воєнного стану щодо захисту персональних даних передбачає розробку системи правових норм, запровадження системи організаційно-технічних заходів та визначення кола посадових осіб, відповідальних за безпечну обробку персональних даних.