Щодо захисту персональних даних в умовах воєнного стану

1. Щодо обмежень прав людини та правових підстав для обробки персональних даних державними органами

Відповідно до частин першої, другої статті 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією 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.

Водночас статтею 64 Конституції України передбачено, що в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень.

Указом Президента України від 24.02.2022 № 64/2022 (далі – Указ) в Україні введено воєнний стан.

Згідно з пунктом 3 Указу 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, зокрема, статтею 32 Конституції України.

Це узгоджується із положеннями статті 8 Конвенції про захист прав людини і основоположних свобод, згідно з якою органи державної влади не можуть втручатись у здійснення права на повагу до приватного і сімейного життя, 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. Також відповідно до статті 15 цієї Конвенції під час війни або іншої суспільної небезпеки, яка загрожує життю нації, будь-яка Висока Договірна Сторона може вживати заходів, що відступають від її зобов'язань за цією Конвенцією, виключно в тих межах, яких вимагає гострота становища, і за умови, що такі заходи не суперечать іншим її зобов'язанням згідно з міжнародним правом.

У статті 9 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних передбачено, що відхилення від положень статей 5 (Якість даних), 6 (Особливі категорії даних) та 8 (Додаткові гарантії для суб'єкта даних) цієї Конвенції дозволяється тоді, коли таке відхилення передбачене законодавством Сторони та є в демократичному суспільстві необхідним заходом, спрямованим на:

a) захист державної та громадської безпеки, фінансових інтересів Держави або на боротьбу з кримінальними правопорушеннями;

b) захист суб'єкта даних або прав і свобод інших людей.

Закон України «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, також містить положення, що стосуються обмеження його дії.

У статті 25 цього Закону передбачено, що обмеження дії статей 6 (Загальні вимоги до обробки персональних даних), 7 (Особливі вимоги до обробки персональних даних) і 8 (Права суб'єкта персональних даних) цього Закону може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

Загальновідомо, що обробка персональних даних має ґрунтуватись на меті та правових підставах.

Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

Відповідно до статті 11 Закону України «Про захист персональних даних» підставами для обробки персональних даних є:

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

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

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 законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

Варто зауважити, що згода суб'єкта персональних даних є лише однією з шести правових підстав для обробки персональних даних, передбачених статтею 11 Закону України «Про захист персональних даних». За наявності підстав, визначених пунктами 2-6 частини першої статті 11 цього Закону, обробка персональних даних здійснюється без згоди суб'єкта персональних даних.

Згідно із Законом України «Про правовий режим воєнного стану» воєнний стан передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності.

Водночас відповідно до частини другої статті 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

У такому випадку підставами для обробки (збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення, знеособлення, знищення тощо) персональних даних відповідними державними органами та органами місцевого самоврядування є пункти 2 та 5 частини першої статті 11 Закону України «Про захист персональних даних», а саме:

- дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;
- необхідність виконання обов'язку володільця персональних даних, який передбачений законом.

Крім того, передбачена у статті 7 Закону України «Про захист персональних даних» заборона на обробку 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 не застосовується, якщо обробка персональних даних, зокрема, стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом.

Таким чином, в умовах введеного в Україні воєнного стану захист персональних даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних, захист державних інформаційних ресурсів, ІТ-систем об'єктів критичної інфраструктури, державних реєстрів, які містять персональні дані є вкрай важливими. Обробка персональних даних має здійснюватися з урахуванням викладених вище положень законодавства України. Така обробка має бути пропорційною та здійснюватися для конкретних і законних цілей.

2. Щодо обов'язків володільців та розпорядників персональних даних стосовно забезпечення захисту персональних даних

Органи державної влади, органи місцевого самоврядування, підприємства, установи і організації усіх форм власності, фізичні особи – підприємці, фізичні особи, що провадять незалежну професійну діяльність, які обробляють персональні дані, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Варто зауважити, що використання персональних даних здійснюється у разі створення умов для захисту цих даних.

Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

Такі обов'язки визначені у статтях 10, 24 Закону України «Про захист персональних даних», які стосуються питань використання персональних даних та забезпечення захисту персональних даних.

Також відповідно до Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 (далі – Типовий порядок), володільці, розпорядники персональних даних самостійно визначають порядок обробки

персональних даних, враховуючи специфіку обробки персональних даних у різних сферах, відповідно до вимог, визначених Законом України «Про захист персональних даних» та Типовим порядком.

Обов'язково мають бути вжиті заходи щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

Володільці, розпорядники персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних та інформаційної безпеки.

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.

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.

Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

З метою забезпечення безпеки обробки персональних даних володільцями, розпорядниками вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

Отже, у разі здійснення обробки персональних даних необхідно створити належні умови для їх захисту.

3. Щодо правових підстав для обробки персональних даних підприємствами, установами і організаціями приватної форми власності, фізичними особами – підприємцями, фізичними особами, що провадять незалежну професійну діяльність з метою надання адресної благодійної допомоги громадянам, які постраждали від військової агресії

Серед правових підстав для обробки персональних даних, які визначені у частині першій статті 11 Закону України «Про захист персональних даних», у даному випадку необхідно виділити: згоду суб'єкта персональних даних на обробку його персональних даних (пункт 1); 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 (пункт 3); захист життєво важливих інтересів суб'єкта персональних даних (пункт 4).

По своїй суті така підстава для обробки персональних даних як захист життєво важливих інтересів суб'єкта персональних даних може застосовуватись у виключних випадках за умови об'єктивної неспроможності особи надати згоду на обробку персональних даних (наприклад, перебування без свідомості) у поєднанні з необхідністю надати їй допомогу для захисту її життєво важливих інтересів.

Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

Згода суб'єкта персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-комунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки.

Враховуючи викладене, згода на обробку персональних даних має відповідати таким вимогам:

✓ добровільність – означає відсутність прямого або опосередкованого примусу при її наданні;

✓ поінформованість – означає, що перед наданням згоди суб'єкт повинен отримати достовірну інформацію про те, ким, з якою метою будуть оброблятися його персональні дані, кому будуть передаватися, які саме дані, а також про права, визначені Законом;

✓ форма надання згоди може бути будь-якою – означає, що умови згоди на обробку персональних даних можуть бути викладені у формі єдиного письмового документа, викладеного доступною для суб'єкта персональних даних мовою, що підписується ним особисто або його законним представником, у електронній формі проставивши відмітку про надання згоди, або ж навіть усно. Водночас надана згода не повинна викликати сумнівів в її однозначності і володілець повинен мати змогу підтвердити її наявність упродовж усього часу здійснення обробки персональних даних.

Разом з тим необхідно враховувати пропорційність обсягу персональних даних суб'єкта. Оброблятися повинні лише ті дані, обробка яких необхідна для досягнення мети. Все залежить від критеріїв, за якими відбувається надання матеріальної чи іншої благодійної/гуманітарної допомоги (категорії суб'єкта, стану здоров'я, матеріального забезпечення, сімейного статусу, кількості дітей тощо).

Отже, якщо для надання адресної благодійної допомоги необхідно здійснювати обробку персональних даних, то варто відповідально підійти до питання оформлення правовідносин та забезпечити захист персональних даних.

4. Щодо захисту своїх персональних даних від кіберзлочинців

За численними повідомленнями в засобах масової інформації громадяни України постійно піддаються хакерським атакам з боку ворожих кіберзловмисників.

Мають місце надсилання електронних листів, повідомлень у месенджерах від начебто державних органів, банків, служби безпеки тощо з рекомендаціями перейти за вказаними у листах/повідомленнях посиланнями. Після завантаження вкладеного файлу зловмисники мають змогу отримати доступ до персональних даних, що містяться на

електронному пристрої користувача (контактів телефонної книги, файлів персонального комп'ютера тощо).

Щоб не стати жертвою кіберзловмисників необхідно уважно ставитись до електронних листів від незнайомих адресатів, повідомлень у месенджерах (Viber, Telegram, WhatsApp) з невідомих номерів телефону, а також повідомлень в соціальних мережах (Facebook) від незнайомих користувачів.

У разі їх надходження не відкривати підозрілі посилання та не завантажувати вкладені файли. Відкриття таких посилань або файлів може спричинити завантаження шкідливого програмного забезпечення на пристрій і отримання доступу до персональних даних.

Необхідно користуватись перевіреними джерелами інформації – наразі це офіційні сторінки державних органів України, які оприлюднюють інформацію та посилання на сервіси щодо знаходження прихистку, розшуку зниклих, отримання допомоги, проведення евакуації тощо.

Щоб вберегти свої персональні дані рекомендується зробити резервні копії документів, фото, телефонної книги, які необхідно зберігати у надійному місці.

Також доцільно виписати номери телефонів найближчих членів родини. Це допоможе не втратити зв'язок з найдорожчими навіть якщо буде втрачено контроль над пристроєм.

5. Щодо захисту своїх персональних даних від шахрайських дій

Під час здійснення парламентського контролю за додержанням законодавства про захист персональних даних виявлено факти шахрайських дій під виглядом виплати грошової допомоги українцям під час воєнного стану.

Такий вид шахрайства як «фішинг в інтернеті», який полягає у крадіжці персональних даних за допомогою підставних веб-сайтів, залишається актуальною проблемою в умовах воєнного стану.

Суть фішингу в тому, що ошукана особа повідомляє дані про себе добровільно. Разом із тим, зловмисник у цьому випадку відіграє роль уповноваженої особи державного органу або благодійного фонду тощо.

Тепер під виглядом надання державних виплат зловмисники виманюють гроші у громадян також шляхом направлення повідомлень.

Як це працює?

• Зловмисники здійснюють розсилку електронних листів, повідомлень у месенджерах (Viber, Telegram, WhatsApp), повідомлень в соціальних мережах (Facebook), SMS-повідомлень, де інформують про виплату матеріальної допомоги вимушеним переселенцям.

• Такі повідомлення містять заклик перейти за наданим гіперпосиланням на певний веб-сайт та заповнити персональні дані (ПІБ, телефон, електронну адресу, реквізити банківських карток тощо) для отримання грошової допомоги.

• Після цього шахраї отримують передані особою персональні дані та привласнюються собі кошти.

Щоб не стати жертвою зловмисників необхідно уважно ставитись до отриманих повідомлень і не розголошувати свої персональні дані на сумнівних, неперевірених веб-сайтах.

6. Щодо можливої загрози для громадян при наданні персональних даних на тимчасово окупованих територіях

Громадянам України, які перебувають на тимчасово окупованих територіях, необхідно бути обережними зі своїми персональними даними.

Центр протидії дезінформації при РНБО України повідомив про нові підступні дії окупанта, які полягають у зборі персональних даних містян під приводом «перепису населення» або під час роздачі «гуманітарної допомоги» для подальшого їх переслідування і залякування.

Це насамперед може стосуватись військовослужбовців, членів їх сімей, а також громадських активістів, журналістів та культурних діячів.

Саме тому необхідно відповідально і свідомо ставитися до безпеки своїх персональних даних і даних своїх близьких та знайомих.

У випадку виникнення підозрілої ситуації чи подібних випадків громадяни можуть поінформувати правоохоронні органи: гаряча лінія Служби безпеки України – 0800 50 14 82, гаряча лінія Національної поліції України – 0800 50 02 02. Також можна звертатися на гарячу лінію Уповноваженого – 0800 50 17 20.