РЕКОМЕДАЦІЇ
щодо забезпечення захисту персональних даних в умовах воєнного стану

Введення на території України правового режиму воєнного стану внесло певні корективи до процедури збирання, обробки, доступу та зберігання персональних даних, як з боку самих суб'єктів персональних даних, так і органів державної влади та місцевого самоврядування.

Незважаючи на встановлені вимоги щодо локалізації даних, органам державної влади надано можливість, серед іншого, розташовувати інформаційні ресурси, публічні реєстри та їхні резервні копії на хмарних ресурсах або в центрах обробки даних, що розташовані за межами України.

Крім того, у зв'язку зі зростаючою загрозою цілісності даних, було прийнято рішення про обмеження або закриття доступу до більшості державних реєстрів.

З метою захисту інформації та державних інформаційних ресурсів **Кабінетом Міністрів України прийнято постанову від 12 березня 2022 року № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану»** (далі – Постанова).

Відповідно до вищевказаної Постанови на період дії воєнного стану міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями (держателями) та/або адміністраторами яких вони є, захисту інформації, що обробляється в них, а також захисту державних інформаційних ресурсів, можуть вживати таких додаткових заходів:

- розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або в центрах обробки даних, що розташовані за межами України, та реєструвати доменні імена у домені gov.ua для такого розміщення;

- створювати додаткові резервні копії державних інформаційних ресурсів та публічних електронних реєстрів з дотриманням установлених для таких ресурсів вимог щодо цілісності, конфіденційності та доступності;

- зберігати резервні копії державних інформаційних ресурсів та публічних електронних реєстрів у зашифрованому вигляді, зокрема за межами України, на хмарних ресурсах та/або окремих фізичних носіях, та/або в ізольованому сегменті центрів обробки даних з дотриманням установлених для таких ресурсів вимог щодо цілісності, конфіденційності та доступності;

- зупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів.

Окрім того, заборонено використання хмарних ресурсів та/або центрів обробки даних, розташованих на тимчасово окупованій території України, або тих, що належать державі, визнаній Верховною Радою України державою-агресором чи державою-окупантом, або належать державі чи суб'єктам, діяльність яких підпадає під дію Закону України «Про санкції», щодо яких прийнято рішення про застосування санкцій в Україні та/або іншій державі та на територіях держав, які входять до митних та воєнних союзів з такими державами.

Також, постановою передбачено припинення здійснення цих заходів протягом шести місяців після припинення чи скасування воєнного стану.

Щодо організації правомірного збирання персональних даних суб'єктами владних повноважень наголошується:

- збирання персональних даних повинне здійснюватися суб'єктами владних повноважень на підставах, в межах їхніх повноважень і способами передбаченими законом;

- збирання персональних даних повинно здійснюватися з використанням автоматизованих інформаційно-телекомунікаційних систем, реєстрів, баз даних з урахуванням повноважень щодо доступу посадових осіб конкретних органів державної влади та місцевого самоврядування;

- крім випадків, прямо передбачених законодавством України (здійснення негласних слідчих розшукових дій, затримання особи, яка підозрюється у вчиненні злочину, виконання інших кримінально-процесуальних заходів), суб'єкт владних повноважень повинен повідомляти суб'єкта персональних даних про склад та зміст зібраних персональних даних, права таких суб'єктів, визначені у частині 2 статті 8 Закону, мету збору персональних даних та осіб, яким передаються його персональні дані;

- первинними джерелами, з яких повинні збиратися персональні дані є документи, видані на ім'я фізичних осіб;

- склад та види персональних даних, які можуть збиратися суб'єктами персональних даних повинні бути пропорційними та ненадмірними стосовно мети їхньої обробки;

- збирання персональних даних має здійснюватися з урахуванням вимог до технічного захисту інформації, забезпечення належного рівня кібербезпеки публічних реєстрів, баз даних, де передбачається обробка персональних даних.

У період дії режиму воєнного стану використання персональних даних має відповідати наступним критеріям:

- ґрунтуватися на передбачених у ст. 11 Закону України «Про захист персональних даних» підставах;

• бути ненадмірними стосовно мети з якою вони використовуються;

• використовуватися лише тими суб'єктами владних повноважень, підприємствами, установами чи організаціями, яким законодавством України надано дозвіл на таку обробку, або відповідною згодою суб'єкта персональних даних;

• бути строковим, тобто здійснюватися протягом періоду, визначеного законодавством України;

• збиратися з достовірних джерел та не надаватися третім особам, без згоди суб'єктів персональних даних та за умови, що запитувачі персональних даних гарантують ступень захисту відповідної інформації на рівні, не гіршому, ніж це робить володілець.

Необхідно звернути увагу, що при визначенні меж правомірного *використання персональних даних* суб'єктами владних повноважень у період дії правового режиму воєнного стану слід враховувати вимоги частини 2 статті 19 Конституції України, а також керуватися завданнями діяльності кожного з таких суб'єктів та змістом повноважень, якими вони наділяються у період дії правового режиму воєнного стану.

Отже, важливо щоб усі учасники правовідносин, пов'язаних із збиранням, обробкою, доступом, зберіганням та захистом персональних даних, як з боку самих суб'єктів персональних даних, так і органів державної влади та місцевого самоврядування, дотримувалися встановлених законодавством вимог у вказаній сфері.

ДМДПЛ МВС