Вх. №25
від 24.02.11р

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ

Україна, 01001, м. Київ
вул. Городецького, 13
Тел./факс: (38-044) 278-37-23

21.02.2011 № 1202-0-26-11

На № _____

Інтернет Асоціація України

01025, м. Київ,
вул. Олеся Гончара, 15/3, офіс 22

Міністерство юстиції України у відповідь на лист Інтернет Асоціації України №7 від 19.01.2011 щодо надання роз'яснень стосовно практичного застосування положень Закону України «Про захист персональних даних» надає інформацію про результати опрацювання вказаного документу.

Додаток: вказане на 6 арк.

Перший заступник Міністра **І.І. Ємельянова**

Інформація

щодо надання роз'яснень стосовно практичного застосування положень Закону України «Про захист персональних даних»

1. ***Яка мінімальна сукупність відомостей дає можливість конкретно ідентифікувати особу та складає собою суть визначення «персональні дані» згідно ст. 2 Закону України «Про захист персональних даних»? У разі, якщо існують кілька окремих сукупностей персональних відомостей, які дають можливість конкретно ідентифікувати особу, просимо надати інформацію по кожній з цих сукупностей.***

Наведене в Законі України «Про захист персональних даних» визначення терміну «персональні дані» в повній мірі відповідає визначенню вказаного терміну, передбаченого в Конвенції Ради Європи про захист осіб у зв'язку із автоматизованою обробкою персональних даних.

Крім того, діючі правові інструменти Європейського союзу у сфері захисту персональних даних спрямовуються на захист фундаментальних прав фізичних осіб, та зокрема їх прав на захист персональних даних, що відповідає Хартії основних прав Європейського Союзу.

Відповідно до міжнародних стандартів термін «персональні дані» повинен охоплювати **всю інформацію про особу, яка ідентифікована або може бути ідентифікована будь яким чином. Для визначення факту ідентифікації особи необхідно враховувати всі засоби, що використовується володільцем або розпорядником баз персональних даних для ідентифікації вказаної особи.**

Такий широкий підхід до визначення персональних даних надає змогу досягти достатньої гнучкості, що дозволяє використовувати вказаний термін у різноманітних ситуаціях та інформаційних і телекомунікаційних ресурсах, які не існували на момент прийняття Конвенції, або можуть виникнути у майбутньому.

2. ***Які умови щодо забезпечення захисту персональних даних у базах персональних даних від незаконної обробки, а також від незаконного доступу до них відповідно до ст. 10 та ст. 24 Закону України «Про захист персональних даних» повинен створити суб'єкт відносин, пов'язаних із персональними даними (володілець, розпорядник бази персональних даних)?***

Володілець бази даних повинен створити умови для захисту персональних даних та забезпечити захист цих даних від незаконної обробки, а також від незаконного доступу до них.

Умови для захисту персональних даних залежать від конкретних реальних загроз, природи персональних даних, які обробляються, технології обробки інформації та типу інформаційної системи, у рамках якої обробляються персональні дані.

У кожному випадку володілець може провести детальний аналіз загроз та інших факторів, які впливають на рівень ризику. На основі аналізу ризиків Володілець може вирішити, який рівень захищеності бази персональних даних є необхідним для створення умов щодо захисту персональних даних.

Слід зазначити, що забезпечення умов для захисту персональних даних у базах персональних даних не вирішується реалізацією визначеної сукупності заходів, а є постійним процесом, який зазвичай включає:

- Розробку політики захисту персональних даних, виходячи з характеристик бізнесу організації, цілей, процесів та процедур суттєвих для управління ризиком небажаних подій щодо обробки персональних даних з урахуванням серйозності наслідків таких небажаних подій. Політика захисту персональних даних повинна бути узгоджена з загальною політикою інформаційної безпеки Вашої організації та з контекстом стратегічного управління ризиками організації.
- Впровадження та забезпечення функціонування політики захисту персональних даних, заходів, процесів та процедур захисту персональних даних;
- Оціннювання і, за можливості, вимірювання продуктивності процесів захисту персональних даних згідно з прийнятою політикою, цілями і практичним досвідом, підготовка пропозицій щодо коригувальних заходів.
- Вживання коригувальних та запобіжних дій щодо захисту персональних даних на підставі результатів внутрішніх перевірок, періодичний перегляд політики захисту персональних даних, постійне удосконалення заходів, процесів та процедур.

Згідно з практикою країн Європейського Союзу заходи щодо забезпечення захисту персональних даних розглядаються як складова частина системи управління інформаційною безпекою організації.

Порядок розробки, впровадження, оцінювання та удосконалення системи інформаційної безпеки організації в Україні, зокрема, визначено стандартом Національного банку України: СОУ Н НБУ 65.1 СУІБ 1.0:2010. Стандарт організації України. Настанова. Методи захисту в банківській діяльності. Система Управління інформаційною безпекою. Вимоги. (ISO/IEC

27001:2005, MOD). Інформаційні технології. Методи захисту.Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)

Оцінка ризиків небажаних подій щодо захисту персональних даних можна здійснювати з урахуванням державного стандарту:ДСТУ ISO/IEC TR 13335-2003. Інформаційні технології.. Настанови з керування безпекою інформаційних технологій. Ч.2. Керування та планування безпеки.

Слід зазначити, що на виконня вимоги пункту.10 статті 6 Закону України «Про захист персональних даних» Державною службою України з питань захисту персональних даних буде опрацьвано документи типового порядоку обробки персональних даних у базах персональних даних. Типовий порядок передбачає класифікацію баз персональних даних за групами ризику, особливості обробки персональних даних у спеціалізованих інформаційних системах, настанови з впровадження заходів щодо захисту персональних даних, аудиту ефективності впроваджених заходів, тощо.

Зазначені документи, згідно з законодавством будуть обговорюватись за участю громадськості, та затверджуватись, у тому числі, з урахуванням Ваших пропозицій та зауваженнь.

Згідно з законом України «Про захист персональних даних» професійні об'єднання можуть розробляти корпоративні кодекси поведінки з метою забезпечення ефективного захисту прав суб'єктів персональних даних, сприяння додержанню законодавства, враховуючи специфіку обробки персональних даних у різних сферах. Вважаємо, що розробка такого кодексу поведінки Інтернет Асоціацією України сприла б досягненню цілей статутної діяльності учасників Асоціації та забезпеченню прав суб'єктів персональних даних.

Вважаємо, що створення умов щодо забезпечення захисту персональних даних у базах персональних даних від незаконної обробки, а також від незаконного доступу до них відповідно до статті 10 та статті 24 Закону України «Про захист персональних даних», у яких ризик небажаних подій є низьким (публічні бази персональних даних) або базовим, не буде вимагати складних та витратних заходів. Для баз даних із підвищеними рівнями ризику впровадження заходів із захисту персональних даних вимагає ретельного опрацювання, фінансових витрат та часу, а для частини володільців – залучення профільних спеціалістів чи співвиконавців.

3. ***Що є предметом контролю за додержанням законодавства про захист персональних даних суб'єктом відносин, пов'язаних із персональними даними (володільцем, розпорядником бази персональних даних), який має здійснюватись відповідно до ст. 22 Закону України «Про захист персональних даних»?***

В державах Європейського Союзу органи нагляду, відповідальні за забезпечення дотримання заходів, які передбачено внутрішньодержавним правом цих країн, мають, зокрема, повноваження стосовно розслідування та втручання, а також право брати участь у судовому розгляді або повідомляти компетентним судовим органам про порушення положень внутрішньодержавного права.

Відповідні повноваження уповноваженого державного органу з питань захисту персональних даних визначено Законом України «Про захист персональних даних». Державна служба України з питань захисту персональних даних здійснює в межах своїх повноважень контроль за додержанням вимог законодавства про захист персональних даних, видає обов'язкові до виконання законні вимоги (приписи) про усунення порушень законодавства про захист персональних даних.

Предметом контролю є додержання вимог законодавства про захист персональних даних суб'єктами відносин пов'язаних із персональними даними, зокрема щодо:

1. Сумлінності та законності обробки даних, тобто:

а) наявності хоча б однієї з визначених нижче умов обробки персональних даних, що відповідають загальним вимогам:

згоди суб'єктів персональних даних на обробку їх персональних даних (стаття 11 пункт 1 абзац 1);

дозволу на обробку персональних даних, що наданий володільцю бази персональних даних відповідно до закону виключно для здійснення його повноважень (стаття 11 пункт 1 абзац 2);

необхідності обробки персональних даних для захисту життєво важливих інтересів суб'єктів персональних даних без їх згоди; а також отримання такої згоди, коли це стало можливим (стаття 6 пункт 7);

необхідності обробки персональних даних у випадках, визначених законом, в інтересах економічного добробуту та прав людини(стаття 6 пункт 6);

необхідності обробки персональних даних у випадках, визначених законом, в інтересах національної безпеки (стаття 6 пункт 6), або:

б) наявності хоча б однієї з визначених нижче умов обробки даних, що відповідають особливим вимогам:

надання суб'єктом персональних даних однозначної згоди на обробку даних, що відповідають особливим вимогам (стаття 7 пункт 1);

необхідності обробки персональних даних, що відповідають особливим вимогам, для здійснення прав та виконання обов'язків у сфері трудових правовідносин відповідно до закону (стаття 7 пункт 2);

необхідності обробки персональних даних, що відповідають особливим вимогам, для захисту інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних (стаття 7 пункт 3);

здійснення обробки персональних даних, що відповідають собливим вимогам, релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створена 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 (стаття 7 пункт 4);

обробки персональних даних, що відповідають особливим вимогам, але раніше були оприлюднені суб'єктом персональних даних (стаття 7 пункт 8);

необхідності обробки персональних даних, що відповідають особливим вимогам для обґрунтування, задоволення або захисту правової вимоги (стаття 7 пункт 5);

обробки персональних даних, що відповідають собливим вимогам,але стосується обвинувачень у вчиненні злочинів, вироків суду, здійснення державним органом повноважень, визначених законом, щодо виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з терроризмом (стаття 7 пункт 7);

обробки персональних даних, що відповідають особливим вимогам, необхідної в цілях охорони здоров'я, для забезпечення піклування чи лікування за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних (стаття 7 пункт 6);

2. Здійснення обробки персональних даних для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством стаття 6 пункт5).

3 Відповідності та ненадмірності складу та змісту персональних даних стосовно визначеної мети їх обробки (стаття 6 пункт 3);

4.Точності та достовірності оброблюваних персональних даних, а також оновлення їх у разі необхідності (стаття 6 пункт 2);

5. Дотримання прав суб'єкта персональних даних визначених Законом України «Про захист персональних даних», зокрема щодо:

надання доступу до своїх персональних даних, що містяться у відповідній базі персональних даних (стаття 8.пункт 2 абзац 3);

отримання інформації про умови надання доступу до персональних даних, зокрема інформації про третіх осіб, яким передаються його персональні дані, що містяться у відповідній базі персональних даних (стаття 8.пункт 2.абзац 2);

пред'явлення вмотивованої вимоги щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником цієї бази, якщо ці дані обробляються незаконно чи є недостовірними (стаття 8 пункт 2 абзац.6);

незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, захисту від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи (стаття 8 пункт2 абзац 7)

6. Дотримання строків обробки персональних даних (у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються), не більших ніж це необхідно до їх законного призначення (стаття 6 пункт 8);

7. Забезпечення захисту персональних даних від незаконної обробки, а також від несанкціонованого доступу до них, суб'єктами відносин, пов'язаних із персональними(стаття 24 пункт 2).

8. Здійснення передачі персональних даних іноземним суб'єктам відносин, пов'язаних із персональними даними, лише за умов забезпечення належного захисту персональних даних, за наявності відповідного дозволу та у випадках, встановлених законом або міжнародним договором України, у порядку, встановленому законодавством. Дотримання вимог поширення персональних даних виключно з тією метою, з якою вони були зібрані (стаття 29 пункт 3).