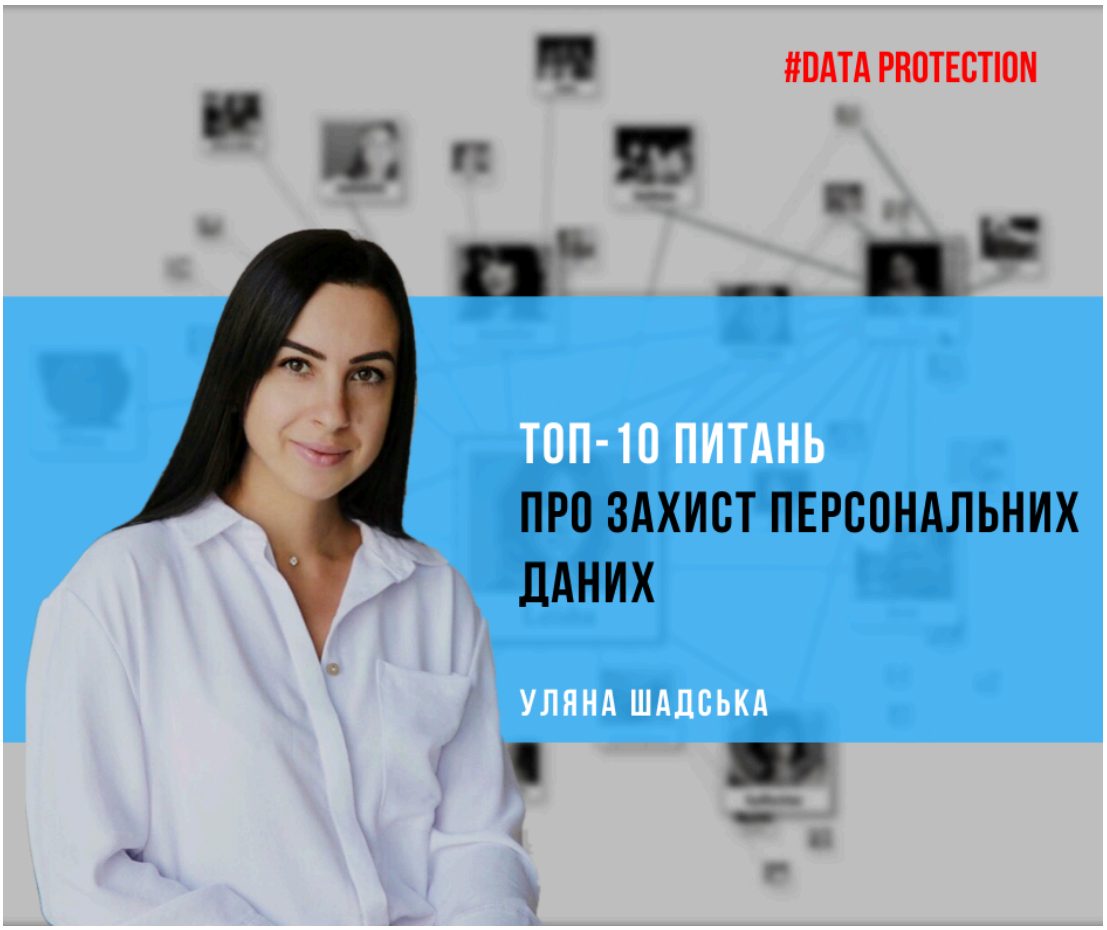
ТОП-10 питань у сфері захисту персональних даних

Дата: 28-10-2019

У 2011 році набрав чинності Закон України «Про захист персональних даних». Його мета – врегулювати правовідносини, пов'язані з обробкою даних та гарантувати право на повагу до приватного і сімейного життя.
Одна з найпоширеніших тез, чому юридичні або фізичні особи не виконують норми Закону: *«Дуже складно розібратися»*. Незнання не позбавляє відповідальності, але потрібно визнати той факт, що законодавство у сфері захисту інформації потребує детального роз'яснення, усвідомлення та адаптації.
У країнах Європейського Союзу докладається максимум зусиль аби населення, державні служби, муніципалітети, бізнес розуміли норми закону, що регулюють обробку даних, кібербезпеку та електронну комунікацію, знали практичні аспекти впровадження та ризики, пов'язані з невиконанням цих положень.



Чи потребує українське суспільство підвищення правосвідомості щодо захисту персональних даних? Відповідь – так. Досить часто до мене

звертаються практично з однаковими питаннями: якими нормативними актами регулюється; на кого поширюються; яка потрібна внутрішня документація; які дані можна збирати, в якому обсязі; хто контролює і т.д.

Потреба в інформації підштовхнула мене підготувати серію матеріалів у форматі «запитання – відповідь». Нижче наведено 10 найпоширеніших питань, які було поставлено протягом року. Варто зауважити, що коротка відповідь не завжди розкриває детальний зміст норми, проте допомагає розібратися в її суті.

Чи поширюється Закон України «Про захист персональних даних» на фізичних осіб?

Так, Закон поширюється на фізичних і на юридичних осіб, які здійснюють будь-які дії, або сукупність дій, таких, як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі, з використанням інформаційних (автоматизованих) систем.

Закон може не застосовуватися, якщо здійснюється обробка даних:

- фізичною особою виключно для особистих чи побутових потреб;
- виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів;
- щодо отримання архівної інформації репресивних органів.

Що таке персональні дані?

Персональні дані – відомості чи сукупність відомостей за допомогою яких фізична особа може бути ідентифікована.

Які є категорії даних?

Людина має фізичну, фізіологічну, соціальну та культурну ідентичність. Персональні дані діляться на дві категорії: загальні та особливі (чутливі).

До загальної категорії можна віднести: прізвище та ім’я; дату та місце народження; громадянство; сімейний стан; псевдонім; дані, записані в посвідченні водія; економічне і фінансове становище; дані про майно; банківські дані; підпис; дані з актів цивільного стану; номер пенсійної справи; адресу місця проживання; дипломи про освіту, професійну підготовку тощо.

Особлива категорія охоплює інформацію про: расове, етнічне та національне походження; політичні, релігійні та світоглядні переконання; членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи громадських організаціях світоглядної спрямованості; стан здоров’я (медичні дані); статеве життя; біометричні дані; генетичні дані; притягнення до адміністративної чи кримінальної відповідальності; застосування до особи заходів у рамках досудового розслідування; вжиття щодо особи заходів, передбачених Законом України «Про

оперативно-розшукову діяльність»; вчинення щодо особи тих чи інших видів насильства тощо.

Що таке обробка даних?

Обробка персональних даних – це будь-яка дія від збирання до знищення персональних даних. Тобто і реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання, поширення (розповсюдження, реалізація, передача), знеособлення тощо (стаття 2 Закону України «Про захист персональних даних»)

Чи потрібно враховувати категорію даних під час їх обробки?

Обов'язково. Під час обробки даних необхідно враховувати їх категорію та застосовувати відповідні рівні безпеки. Більше того, у разі обробки даних, які становлять ризик для прав і свобод людини (особливої категорії даних), розпорядники персональних даних повинні повідомити Уповноваженого Верховної Ради України з прав людини про структурний підрозділ або відповідальну особу, яка організовує роботу з даними.[1] Порядок, яким чином потрібно повідомляти Уповноваженого з прав людини, можна ознайомитися на офіційному сайті.

Що таке внутрішні політики безпеки даних?

Це внутрішні положення (інструкції), які регулюють процедури обробки персональних даних. Вони повинні розроблятися власниками та розпорядниками персональних даних, відповідно до вимог Закону, зважаючи на:

- специфіку діяльності (правові підстави);
- мету обробки, обсяг даних та їх категорії;
- інформаційні системи, мережі, програми, задіяні у процес обробки персональних даних;
- число осіб, які мають доступ до персональних даних (працюють з даними);
- форми ведення реєстру, в якому обробляються персональні дані (мануальна, електронна або змішана);
- ризики, які можуть виникнути при обробці даних, як для систем, так і осіб, чиї дані обробляються тощо.

Що має включати така документація?

Документація, що стосується політики безпеки персональних даних, повинна бути повною, регулярно оновлюватися й містити, як мінімум, інформацію про:

- мету, обсяг, підстави (межі повноважень) обробки персональних даних;
- конфігурацію інформаційної системи (банків даних), мережі, програми тощо;
- номенклатуру оброблюваних персональних даних (види та категорії), їхні локалізації та операції, що проводяться з ними;
- механізм здійснення заходів безпеки (у тому числі, фізичного середовища інформаційних систем);

- докладний опис критеріїв, відповідно до яких будуть доступні персональні дані;
- управління доступом та список авторизованих користувачів (у числі, рівні доступу);
- графік перевірок безпеки та звіти про інциденти безпеки;
- особу, відповідальну за політику безпеки;
- аудит безпеки (графік перевірок та звіти про інциденти безпеки);
- порядок доступу до персональних даних третіх осіб;
- строки збереження, процедури видалення або знищення даних;
- заходи з виявлення випадків несанкціонованого доступу і/або несанкціонованої обробки персональних даних та інш.

Володілець і розпорядник персональних даних, у чому різниця?

Володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Розпорядник персональних даних – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

ПРИКЛАД:
У статті 25 Закону України «Про Національну поліцію» визначено, що поліція в рамках інформаційно-аналітичної діяльності: формує та користується базами (банками) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України. Тобто, володільцем баз даних – буде Міністерство внутрішніх справ України, а розпорядником – Національна поліція.

Що таке згода суб'єкта персональних даних?

Згода суб'єкта персональних даних – 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-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки (стаття 2 Закону України «Про захист персональних даних»).
Із зазначеного вбачається, що можна виділити декілька способів отримання згоди від особи:

1) Згода надана у письмовому/електронному вигляді.
2) Усна згода. Особа може в усній формі виразити свою згоду.

3) Мовчазна згода. Коли особа була попереджена, але не виразила своїх заперечень.

ВАЖЛИВО!

Окремо варто звернути увагу на отримання згоди від неповнолітніх, малолітніх чи недієздатних осіб. В таких випадках необхідно отримувати згоду від тих осіб (наприклад, батьків, опікунів чи усиновителів), які повністю усвідомлюють значення дій та наслідків, які можуть статися під час обробки даних. Відповідно до статті 10 Закону України «Про охорону дитинства», розголошення чи публікація будь-якої інформації про дитину, що може заподіяти їй шкоду, без згоди законного представника дитини **забороняється.**

Які законодавчі акти гарантують право людини на захист даних?

1. Конституція України (стаття 32).
2. Загальна Декларація прав людини (стаття 12).
3. Міжнародний Пакт про громадянські і політичні права (стаття 17)
4. Конвенція про захист прав людини і основоположних свобод (стаття 8).
5. Конвенція Ради Європи про захист осіб у зв'язку автоматичною обробкою персональних даних.
6. Закон України «Про захист персональних даних».
7. Витяг з Кодексу України про адміністративні правопорушення (стаття 188-39 «Порушення законодавства у сфері захисту персональних даних», стаття 188-40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»).
8. Витяг з Кримінального кодексу України (стаття 182 «Порушення недоторканності приватного життя»).
9. Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 № 1/02-14.

Звісно, що цей перелік не вичерпний. Далі ми продовжимо висвітлювати нормативні документи та законодавчі рішення.

Автор: Уляна Шадська
#dataprotection

Уляна Шадська, Керівниця програм "Безпека громад" та "Право на приватність"
0

Warning: file_get_contents(http://graph.facebook.com/?id=https://ecpl.com.ua/experts/ulyana-shadska/): failed to open stream: HTTP request failed! HTTP/1.1 400 Bad Request

in **/home/ecpl/ecpl.com.ua/www/wp-content/themes/ecpl2016/functions.php** on line **496**