Інформація
щодо захисту персональних даних
та порядку реєстрації цих баз

1 січня 2011 року набрав чинності Закон України "Про захист персональних даних" (далі - Закон), прийнятий Верховною Радою України 1 червня 2010 року, який регулює відносини, пов'язані із захистом персональних даних під час їх обробки, і поширюється на всіх юридичних та фізичних осіб – володільців бази персональних даних **(в тому числі на будь-яку ланку профспілкової організації – юридичну особу).**

Зазначене ґрунтується на тому, що відповідно до статті 32 Конституції України будь-яка фізична особа не може зазнавати втручання в її особисте життя, отже будь-яка юридична або фізична особа, що є володільцем бази персональних даних зобов'язана гарантувати фізичній особі належний захист її персональних даних шляхом здійснення певних заходів для такого захисту.

З метою дотримання законодавства про захист персональних даних будь-яка юридична особа (**володілець бази персональних даних**) має зробити наступне:

1) самостійно визначити перелік баз даних (їх найменування), які ним обробляються відповідно до Закону з урахуванням цілей обробки персональних даних, сформульованих відповідно до вимого законодавства України, бізнес-процесів володільця, структури, місцезнаходження баз персональних даних, структури інформаційної системи тощо;

2) визначити законні підстави для обробки персональних даних у базах персональних даних;

3) визначити структурний підрозділ або відповідальну особу, яка організовує роботу, пов'язану із захистом персональних баз даних при їх обробці;

4) запровадити процедури доступу до персональних даних працівників відповідно до їхніх професійних або трудових обов'язків та надання ними зобов'язань (гарантій) щодо недопущення розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних або трудових обов'язків;

5) запровадити процедури, спрямовані на забезпечення дотримання принципів обробки персональних даних: законності; сумісності (персональні дані повинні отримуватися із конкретними законними цілями та оброблятися відповідно до них); адекватності і не надлишковості; точності; строковості зберігання; дотримання прав фізичної особи; захищеності;

6) забезпечити захист персональних даних у базі персональних даних від незаконної обробки та незаконного доступу до них. Для цього доцільно розробити Положення про захист персональних даних (у наступній інформації буде наведений зразок такого положення);

7) отримати від працівників письмову згоду на обробку персональних даних (зразок згоди наводився у попередній інформації);

8) повідомити працівника про їхні права у сфері захисту персональних даних, мету обробки персональних даних, осіб, яким передаються дані;

9) привести посадові інструкції працівників кадрової служби, бухгалтерії у відповідність до законодавства про захист персональних даних;

10) оформити заяву про реєстрацію бази персональних даних Зразок наводився у попередній інформації);

11) зареєструвати базу персональних даних у порядку, визначеному Законом та отримати свідоцтво про реєстрацію.

Спочатку необхідно розглянути, що означають деякі терміни, які використовуються для цілей цього Закону, а саме:

"Обробка персональних даних" – будь-яка дія або сукупність дій, здійснених повністю або частково в інформаційній (автоматизованій) системі та/або в картотеках персональних даних, які пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знеособленням, знищенням відомостей про фізичну особу.

Приймаючи особу на роботу або укладаючи цивільно-правовий договір на виконання робіт (надання послуг), юридична особа отримує від особи паспортні дані, ідентифікаційний код, у необхідних випадках – документи про освіту, склад сім'ї, У цьому випадку отримання відомостей і є **збиранням персональних даних про особу.**

Отримані відомості про особу систематизуються і зберігаються в особових картках (типова форма № П-2), особових справах, в інформаційних базах кадрових чи бухгалтерських програм. Це і є **накопичення персональних даних та їх зберігання.** Зберігання персональних даних передбачає запровадження процедури доступу до цих даних працівників відповідно до їхніх професійних або трудових обов'язків та надання цими працівниками зобов'язань (гарантій) щодо недопущення розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних або трудових обов'язків.

Пропонуємо наступний алгоритм дій.

Крок 1. Визначення баз персональних даних.

Відповідно до статті 2 Закону **персональні дані це** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. До таких даних відносяться: паспортні дані, адреса місця реєстрації, номери домашнього та мобільного телефонів, ідентифікаційний код тощо. Слід звернути увагу, що цей термін застосовується лише до **фізичних осіб.**

Фіксуючи персональні дані в первинному порядку на паперових носіях (картотека), електронних носіях або в будь-який інший спосіб, саме і створюється **база персональних даних,** для якої володілець повинен визначити

та затвердити **мету обробки, встановити склад персональних даних та процедури їх обробки.**

У кожній юридичній особі можна виділити кілька баз персональних даних. За наявності найманих працівників буде база персональних даних **"Працівники",** до якої належить картотека особових карток (типова форма № П-2), усі особові справи працівників, довідник з відомостями про працівників у програмі 1С.

Якщо юридична особа при провадженні господарської діяльності має справу з фізичними особами, які виконують роботи (надають послуги) за цивільно-правовими договорами, укладає договори оренди, купівлі-продажу тощо створюється база персональних даних **–"Фізичні особи, персональні дані яких обробляються у ході ведення господарської діяльності".** До цієї бази вносяться персональні дані фізичних осіб – підрядників, контрагентів або персональні дані фізичних осіб, що перебувають у трудових відносинах з іншою юридичною особою – підрядником, контрагентом.

Крім зазначених вище баз персональних даних, у первинній організації профспілки створюється база персональних даних **членів профспілки,** до якої включаються персональні дані членів профспілки, а також осіб, які підтримують з нею постійні контакти у зв'язку з характером їх діяльності.

Крок 2. Визначення мети обробки баз персональних даних.

Слід ще раз нагадати, що **метою обробки персональних даних є забезпечення реалізації:**

- трудових відносин;
- адміністративно-правових (в тому числі, відносин у сфері державного управління), податкових відносин та відносин у сфері бухгалтерського обліку;
- відносин у сфері управління людськими ресурсами, зокрема, кадровим потенціалом;
- відносин у сфері економічних, фінансових послуг та страхування;
- відносин у сфері реклами та збору персональних даних у комерційних цілях;
- відносин у сфері телекомунікаційних послуг;
- відносин у сфері громадської, політичної та релігійної діяльності, культури, дозвілля, спортивної та соціальної діяльності;
- відносин у сфері освіти;
- відносин у сфері охорони здоров’я;
- відносин у сфері безпеки, включаючи питання приватних розслідувань, побудови системи приватної безпеки та приватної охорони;
- відносин у сфері транспорту;
- відносин у сфері науки, історичних досліджень та статистики;
- інших відносин, що вимагають обробки персональних.

Керуючись наведеним, до кожної створеної бази персональних даних визначаємо мету:

База персональних даних **"Працівники"** створюється **з метою забезпечення реалізації трудових відносин, адміністративно-правових, податкових відносин та відносин у сфері бухгалтерського обліку.**

База персональних даних **"Фізичні особи, персональні дані яких обробляються у ході ведення господарської діяльності"** створюється **з метою оформлення з фізичними особами цивільно-правових відносин.**

База персональних даних **членів профспілки** створюється **з метою забезпечення реалізації відносин у сфері громадської діяльності.**

Крок 3. Визначити законні підстави для обробки баз персональних даних.

Персональні дані поділяються на дві категорій за підставами виникнення права на обробку таких даних:

1) згода суб'єкта персональних даних на обробку його персональних даних. Суб'єкт персональних даних має право при наданні згоди внести застереження стосовно обмеження права на обробку своїх персональних даних;

2) право на обробку персональних даних надане володільцю бази персональних даних у порядку, визначеному законодавством України.

Що таке згода суб'єкта персональних даних на обробку його персональних даних?

Згода суб'єкта персональних даних – будь-яке документоване, зокрема, письмове, добровільне волевиявлення фізичної особи щодо надання дозволу володільцю бази персональних даних на обробку її персональних даних відповідно до сформульованої мети їх обробки та передачі їх третій особі.

Документовану згоду на обробку персональних даних слід отримати від усіх працівників, прийнятих на роботу після 1 січня 2011 року(зразок якої наведено у попередній інформації)**.** У подальшому таку заяву слід отримувати від кожного працівника, якого приймають на роботу.

Отримувати заяви від працівників, прийнятих на роботу у попередні роки, не потрібно, оскільки закон не має зворотної дії у часі. Вважається, що обробка персональних даних провадиться на підставі вільного волевиявлення сторони трудового договору відповідно до відносин, що виникли до набрання законом чинності.

Що стосується отримання згоди від інших фізичних осіб, які виконують роботи (надають послуги) для юридичної особи на підставі цивільно-правових договорів доцільно розробити наступний зразок заяви:

Керівнику

_____

(прізвище, ім'я, по батькові
фізичної особи)

Заява

Відповідно до Закону України "Про захист персональних даних" даю згоду на обробку моїх персональних даних з первинних джерел (у т.ч. паспортні дані, ідентифікаційний код) з метою забезпечення реалізації відносин у сфері бухгалтерського обліку.

Дата Підпис фіз.особи

Крок 4. Повідомлення працівників про їхні права у сфері захисту персональних даних, мету обробки персональних даних, осіб, яким передаються дані.

З урахуванням вимог статті 12 Закону працівник, як суб'єкт персональних даних, протягом **10 робочих днів** з дня включення його персональних даних до бази персональних даних має бути повідомлений виключно у письмовій формі (зразок наведений у попередній інформації) про:

свої права, визначені статтею 8 Закону,

мету збору даних (забезпечення реалізації трудових відносин, адміністративно-правових, податкових, відносин в сфері бухгалтерського обліку),

осіб, яким передаються його персональні дані.

Повідомлення не здійснюються, якщо персональні дані збираються із загальнодоступних джерел.

Зібрані відомості про суб'єкта персональних даних, а також інформація про їх джерела надаються цьому суб'єкту, за його вимогою, крім випадків, установлених законом.

Направляти повідомлення працівникам, прийнятим на роботу у попередні роки, не потрібно. У подальшому такі повідомлення надаються кожному працівнику, прийнятому на роботу, у десятиденний строк з дня оформлення особової картки (особової справи) або включення відомостей про працівника до електронної бази даних (бухгалтерська чи кадрова програма, зокрема 1С).

Крок 5. Визначення наявності розпорядника баз персональних даних.

Відповідно до статті 2 Закону **розпорядником бази персональних даних** є фізична чи юридична особа, якій володільцем бази персональних даних або законом надано право обробляти ці дані. Володілець може доручити обробляти персональні дані розпоряднику на підставі письмового договору про це.

У сфері трудових відносин розпорядник буде зустрічатися дуже рідко. Прикладом наявності розпорядника у трудових відносинах може бути наступне. В юридичній особі відсутній відділ кадрів, а кадрове діловодство ведеться сторонньою фірмою (кадровою агенцією), то ця фірма може вважатися розпорядником бази "Працівники".

Крок 6. Внесення змін до установчих документів.

Відповідно до пункту 1 статті 6 Закону мета обробки персональних даних має бути сформульована у законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, та відповідати законодавству про захист персональних даних.

Крок 7. Реєстрація баз персональних даних

Кожна база персональних даних (в електронному вигляді та/або в картотеках, в яких обробляються персональні дані) незалежно від обсягу та форми їх застосування, виду діяльності **підлягає державній реєстрації** шляхом внесення відповідного запису уповноваженим державним органом з питань захисту персональних даних до Державного реєстру баз персональних даних. **Виключень щодо реєстрації баз персональних даних Закон не містить.**

Для реєстрації бази персональних даних уповноваженому державному органу з питань захисту персональних даних **володільцем бази персональних даних (це стосується будь-якої ланки профспілкової організації, що є юридичною особою)** подається заява встановленого зразка **(**зразок наведено у попередній інформації). При цьому, щодо кожної бази даних, яка перебуває у володінні заявника, подається окрема заява**. Первинна профспілкова організація, що не є юридичною особою, не подає заяв на реєстрацію баз персональних даних, якими вона володіє,** однак всі дії щодо захисту персональних даних має

Заява про реєстрацію бази персональних даних повинна містити:

інформацію про володільця бази персональних даних,

інформацію про базу даних та місце її знаходження,

підтвердження зобов’язання стосовно виконання вимог законодавства щодо захисту персональних даних.

Крок 8. Необхідно привести посадові інструкції працівників, на яких покладена обробка персональних даних, і відповідно положення про структурні підрозділи

У першу чергу це стосується посадової інструкції інспектора з кадрів, або іншого спеціаліста, на якого будуть покладені такі обов'язки, та відділ бухгалтерського обліку або бухгалтера (зразки будуть наведені у наступній інформації)ю.

Крок 9. Необхідно отримати від працівників юридичної особи, які обробляють персональні дані, зобов'язання щодо нерозголошення персональних даних.

Відповідно до статті 10 Закону використання персональних даних працівниками суб'єктів відносин має 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. Таке зобов'язання чинне і після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, встановлених законом.

У зв'язку з цим необхідно отримати від працівників, які за посадовими обов'язками мають справу з персональними даними інших осіб, **письмові зобов'язання щодо нерозголошення персональних даних.**

Наводимо зразок такого зобов'язання:

Керівнику

Інспектора кадрів
Прізвище, ім'я, по батькові

Зобов'язання

Відповідно до статті 10 Закону України "Про захист персональних даних" зобов'язуюсь не розголошувати у будь-який спосіб персональні дані інших осіб, у т.ч. працівників (назва юридичної особи), що стали відомі мені у зв'язку з виконанням посадових обов'язків.

Підтверджую, що зобов'язання буде чинним після припинення мною діяльності, пов'язаної з обробкою персональних даних, крім випадків, встановлених законом.

Крок 10. Необхідно розробити положення про захист персональних даних.

Оскільки відповідно до Закону володілець бази персональних даних має забезпечити захист цих даних Державною службою з питань захисту персональних даних розроблений **Типовий порядок обробки персональних даних** (знаходиться на реєстрації в Мінюсті), на підставі якого має бути розроблений локальний нормативний акт в кожній юридичній особі, яким регламентуватиметься процес обробки персональних даних. Одна із основних функцій цього документа – запровадження процедур доступу до персональних даних, що обробляються.

Підсумовуючи наведене, необхідно звернути увагу на рекомендації Державної служби з питань захисту персональних даних щодо дії будь-якої юридичної особи у сфері захисту персональних даних працівників до кінця поточного року, тобто у 2011 році. За цими рекомендаціями юридична особа має видати розпорядчий документ (наказ, розпорядження), у якому зафіксувати дії щодо приведення процесів та процедур обробки персональних даних у відповідність до законодавства у сфері захисту персональних даних. Зразок документу наводиться у **Додатку**.

Департамент правового захисту

Додаток
до Інформації 2

РОЗПОРЯДЖЕННЯ

19.12.2011 м.Київ № 207

Про приведення процесів та процедур обробки персональних даних у відповідність до законодавства

На виконання Закону України "Про захист персональних даних", відповідно до Положення про Державний реєстр баз персональних даних та порядок його ведення, затвердженого постановою Кабінету Міністрів України від 25 травня 2011 р. № 616, наказу Міністерства юстиції України від 8 липня 2011 р. № 1824/5, з метою створення дієвої системи управління персональними даними

1. Утворити робочу групу із запровадження захисту баз персональних даних, що обробляються у діяльності (назва юридичної особи), у складі:

голова групи – П.І.Б., заступник керівника юридичної особи;

члени групи - П.І.Б., представник кадрової служби;
П.І.Б., представник юридичної служби;
П.І.Б., представник бухгалтерії;
П.І.Б., представник відділу інформаційних технологій.

2. Робочій групі:

2.1. До 21.12.2011:

2.1.1. Провести аналіз процесів обробки персональних даних відповідно до основних завдань і функцій.

2.1.2. Відповідно до пунктів 2, 3 статті 6 Закону України "Про захист персональних даних" проаналізувати склад та зміст персональних даних, що обробляються, та визначити, чи є вони надмірними стосовно мети їх обробки.

2.1.3. Визначити мету обробки персональних даних та кількість баз персональних даних, що підлягають державній реєстрації, наявність розпорядників баз.

2.1.4. Результати роботи групи подати (посада керівника) у письмовій формі для погодження.

2.2. Розробити проект Положення про захист персональних даних у (назва юридичної особи).

3. ПІБ, посада підготувати проект змін до (вказується назва установчого документу) щодо формулювання мети обробки персональних даних (вказується назва юридичної особи) (згідно з пунктом 1 статті 6 Закону України "Про захист персональних даних").

4. Кадровій службі до 25.12.2011:

4.1. Забезпечити отримання документованої згоди на обробку персональних даних від працівників (назва юридичної особи).

4.2. Письмово повідомити працівників про права. Визначені законодавством у сфері захисту персональних даних, мету обробки персональних даних та осіб, яким передаються персональні дані, у строки, визначені законодавством.

4.3. Привести посадові інструкції працівників відповідальних за кадрову роботу у відповідність до законодавства про захист персональних даних та подати їх на затвердження.

5. Кадрова служба, юридична служба :

5.1. Визначити перелік посад, виконання обов'язків за якими пов'язано з обробкою персональних даних, підготувати проекти змін до відповідних посадових інструкцій та подати їх на затвердження, погодивши з відповідними керівниками структурних підрозділів.

5.2. Отримати до 25.12. 2011 від працівників, робота яких пов'язана з обробкою персональних даних, письмові зобов'язання щодо недопущення 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.

6. Керівнику робочої групи:

6.1. Організувати роботу з отримання згоди на обробку персональних даних від фізичних осіб, дані яких включаються до баз персональних даних, та забезпечити повідомлення зазначених осіб про права, визначені законодавством у сфері захисту персональних даних, мету обробки персональних даних, осіб, яким передаються дані (за їх наявності).

6.2. Подати заяви про реєстрацію баз персональних даних до Державної служби України з питань захисту персональних даних.

7. Призначити (бажано заступника керівника юридичної особи) відповідальним за організацію роботи, пов'язаної із захистом персональних даних при їх обробці.

8. Контроль за виконанням розпорядження залишаю за собою.

Керівник юридичної особи П.І.Б.