Інструкція з розроблення Політики інформаційної безпеки та роботи з персональними даними

Зміст

Вступ

Політика інформаційної безпеки та роботи з персональними даними є важливим інструментом захисту наявної в неприбутковій організації інформації про саму організацію, її бенефіціарів, працівників та інших залучених осіб.

Неприбуткова організація має гарантувати захист даних, які вона збирає та зберігає на своїх носіях, визначати обмежене коло осіб, які мають доступ до цих даних, регулювати механізми захисту фізичних та електронних даних. Також ця політика повинна регулювати процедуру надання згоди на обробку та зберігання даних, адже жодні особисті дані бенефіціарів чи інших осіб не можуть бути зібрані без їхньої попередньої згоди. Отже, Політика інформаційної безпеки та роботи з персональними даними, базуючись на законодавстві України, гарантує дотримання цього законодавства щодо обробки інформації та поводження з особистими даними.

В першу чергу інформаційна безпека стосується захисту внутрішньої документації організації. Деякі документи організації можуть мати публічний характер, наприклад, статутні документи, бюджети та звіти. Проте організація має регулювати рівень доступу до цих документів, фільтрувати документи, які можуть бути опубліковані, та ті, які призначені для внутрішньої обробки. Це інформація про внутрішні фінансові операції та документи, які містять персональну інформацію про працівників, волонтерів, підрядників, партнерів та інших залучених осіб. Сюди відносяться дані про нарахування заробітної плати, паспортні дані персоналу або залучених осіб, їхні контактні номери, адреси та банківські реквізити тощо. Організація має гарантувати забезпечення належної обробки цих даних та надійного зберігання, аби не сталося витоку цієї інформації за межі кола осіб, які мають право на доступ до неї.

Особливий акцент у цій політиці має бути зроблено на обробці та зберіганні даних бенефіціарів організації. Бенефіціари є сторонніми особами, не дотичними напряму до організації. Вони за власною згодою надають певні особисті дані для використання організацією. Треба також враховувати, що бенефіціарами часто є вразливі категорії населення або діти. Тому важливо не просто отримати формальний дозвіл на обробку їхніх даних, а ще й переконатися, що ці особи повністю розуміють та усвідомлюють, які документи підписують та на що дають згоду. Якщо доросла людина не спроможна надати цей дозвіл чи зрозуміти ситуацію або ви працюєте з дітьми, потрібно сконтактувати із законними опікунами цих осіб щодо оформлення дозволу на обробку даних. Тож ця політика визначає процедури отримання дозволу на обробку персональних даних бенефіціарів та механізми надійного зберігання цих даних.

Отже, Політика інформаційної безпеки та роботи з персональними даними визначає та регулює такі детально розглянуті в цій інструкції процеси в організації:

- Визначення ключових для цієї політики понять щодо інформаційної безпеки та персональних даних, базованих на законодавстві України.

- Визначення механізмів отримання згоди на обробку персональних даних та змісту цієї згоди.

- Управління базами даних організації, які містять персональні дані.

- Механізми реагування на ситуації витоку персональних даних в організації.

- Визначення рівнів доступу до персональних даних в організації та передача доступу третім особами, що базується на Законі України «Про захист персональних даних».

Наприкінці розробленої політики обов'язково має міститися інформація про відповідальних осіб, які задіяні до розроблення цієї політики, а також осіб, які відповідальні за її дотримання в організації. Крім цього, політика має завершуватися затвердженим шаблоном згоди на обробку персональних даних, яким у подальшому організація має послуговуватися під час збору особистих даних окремих осіб.

Підготовка до створення Політики інформаційної безпеки та роботи з персональними даними

Підготовка до створення Політики інформаційної безпеки та роботи з персональними даними має базуватися на послідовному аналізі специфіки діяльності вашої організації, оцінці потреб та основних ризиків безпеки із сильним фокусом на законодавстві України в цій сфері.

Ви можете скористатися шаблоном, на основі якого можна розробити та затвердити Політику інформаційної безпеки та роботи з персональними даними у вашій організації.

Пам'ятайте, що ця політика, як і будь-яка інша, повинна мати специфікацію згідно з потребами саме вашої організації, тому механічне заповнення запропонованого шаблону є недостатнім.

Підготовка до складання Політики інформаційної безпеки та роботи з персональними даними передбачає поетапне здійснення таких дій:

1. Аналіз специфіки діяльності організації

- Визначення груп осіб та структур, з якими працює організація та чиї дані зберігає зараз та буде зберігати в майбутньому. Це можуть бути працівники організації та волонтери, бенефіціари, партнери, підрядники тощо.

- Специфікація інформації, що зберігається. Цей етап передбачає визначення, з якими типами інформації працює організація і які типи інформації зберігаються. Це можуть бути персональні дані осіб, чутлива особиста інформація, внутрішні документи організації тощо.

- Аналіз бенефіціарів — визначення груп бенефіціарів, із якими працює організація, характеристика збереженої інформації про них та рівень доступності для них інформації про зберігання даних. Як було вже зазначено у вступі, якщо ви працюєте з вразливими категоріями населення, тоді мають бути створені особливі передумови та гарантії зберігання їхніх персональних даних та чутливої інформації. Якщо ви взаємодієте з дітьми або з особами, які не здатні зрозуміти інформаційну згоду, потрібно обов'язково контактувати з їхніми офіційними опікунами та узгоджувати інформаційні згоди з ними, адже підписи таких осіб можуть не мати юридичної сили.

- Визначення основних процесів в організації та проєктів, у яких обробляються персональні дані. Цей етап передбачає оцінювання внутрішньої та проєктної діяльності організації та визначення ситуацій, у яких обробляється персональна інформація, яка потребує захисту. Це можуть бути бухгалтерські процеси в організації, складання звітності та бюджетування, здійснення платежів, найом нових співробітників, реєстрація волонтерів, комунікація в соціальних мережах, передача гуманітарної допомоги тощо. Визначте якомога більше процесів усередині організації, які передбачають роботу з персональними даними, адже це дасть змогу визначити ключові ризики і впровадити безпекові механізми для кожного процесу.

- Аналіз наявних способів зберігання персональних даних та чутливої інформації. Цей заключний етап аналізу специфіки діяльності організації передбачає оцінювання наявних на сьогодні інструментів обробки та зберігання інформації. Він включає оцінювання способів зберігання цифрової та паперової інформації й передбачає аналіз захищеності можливих платформ та сховищ для зберігання даних.

2. Визначення потреб організації в інформаційній безпеці

Для визначення потреб організації варто взяти до уваги результати аналізу специфіки діяльності організації та оцінити ймовірність ризиків порушення інформаційної безпеки в тих чи тих сферах діяльності. Оцінка має базуватися на чинних нормах законодавства у сфері захисту персональних даних, зафіксованих у Законах України «Про інформацію» та «Про захист персональних даних».

Тож до кожного пункту специфіки діяльності організації можуть бути поставлені наведені нижче запитання для визначення потенційних ризиків та потреб організації в посиленні інформаційної безпеки.

- Визначення груп осіб та структур, із якими працює організація:

- Хто саме є суб'єктами персональних даних у нашій організації?

- *Чи забезпечуємо ми поінформованість цих осіб про зберігання та обробку їхніх даних?*

- *Чи надають ці суб'єкти письмову згоду на обробку персональної інформації?*

- *Чи зберігаємо ми персональні дані осіб, із якими більше не співпрацюємо?*

- Специфікація інформації, що зберігається:

- *Інформацію яких типів ми збираємо? Чи є серед них чутливі або конфіденційні дані?*

- *Чи справді нам необхідно зберігати всі ці категорії даних?*

- *Чи чітко ми розмежовуємо загальнодоступну, службову й конфіденційну інформацію?*

- Аналіз бенефіціарів, із якими працює організація:

- *Якого характеру інформацію про наших бенефіціарів ми збираємо та обробляємо?*

- *Чи зберігаємо ми особисту та особливо чутливу інформацію про наших бенефіціарів?*

- *Чи доступна та зрозуміла для них процедура надання згоди на обробку персональних даних?*

- *Чи враховуємо ми мовні, когнітивні або вікові особливості під час отримання згоди на обробку персональних даних?*

- *Чи отримуємо ми в належний спосіб згоду на обробку персональних даних від дітей або дорослих осіб, які через різноманітні обставини мають законних опікунів? Чи цікавимося ми наявністю законних опікунів у випадках, коли не впевнені у спроможності бенефіціара самостійно ухвалити рішення?*

- Визначення основних процесів, у яких обробляються персональні дані:

- *Які саме внутрішні процеси в нашій організації потребують уваги до захисту інформації?*

- *Яка програмна діяльність нашої організації передбачає* збір *та обробку персональних даних?*

- *Чи всі учасники цих процесів (працівники, волонтери та інші залучені особи) розуміють вимоги щодо безпеки даних? Чи в належний спосіб вони поінформовані про безпеку даних?*

- *Чи передаємо ми персональні дані третім сторонам (підрядникам, партнерам)? І чи це оформлено належно?*

- *Які ризики для безпеки даних пов'язані з кожним процесом?*

● Аналіз наявних способів зберігання персональних даних:

- *Де зберігаються персональні дані: на папері, на локальних комп'ютерах, на хмарних сервісах?*

- *Чи захищене фізичне місце зберігання паперових документів?*

- *Чи мають працівники різні рівні доступу до інформації? Чи ми встановлюємо коло відповідальних осіб, які мають обмежені рівні доступу до тих чи тих даних?*

- *Чи використовуються захищені паролі, шифрування, резервне копіювання?*

- *Як ми контролюємо доступ до інформації після звільнення працівника?*

- *Які є ризики витоку інформації за наявних нині способів зберігання даних у нашій організації?*

3. Визначення законодавчих вимог та міжнародних стандартів

Цей етап передбачає визначення законодавчого підґрунтя для формування Політики інформаційної безпеки та роботи з персональними даними. Як було зазначено вище, в українському законодавстві є закони, які визначають поняття та регулюють питання інформаційної безпеки. Це Закони України «Про інформацію» та «Про захист персональних даних». Саме на цих двох документах має базуватися розроблена вами політика.

Також радимо звернути увагу на міжнародні норми регулювання захисту даних, особливо якщо ви співпрацюєте з міжнародними донорами та партнерами. В такому випадку наявність міжнародних стандартів може бути не тільки вимогою ваших донорів, а й зрозумілою формою регулювання взаємовідносин із партнерами на міжнародному рівні.

У цьому разі можна послуговуватися, зокрема, GDPR (General Data Protection Regulation). Це Загальний регламент захисту даних Європейського Союзу. Цей документ визначає загальні принципи та правила щодо згоди на обробку і збереження персональних даних, механізми захисту даних та шляхи реагування у випадках витоку даних резидентів Європейського Союзу.

4. Визначення відповідальних за політику осіб

Визначення відповідальних за Політику інформаційної безпеки та роботи з персональними даними осіб — це ключовий етап її підготовки та впровадження. Мета цього етапу — чітко окреслити, хто саме в організації відповідає за створення, впровадження, моніторинг та оновлення політики, а також за дотримання вимог щодо захисту персональних даних.

Важливо пам'ятати, що у випадку Політики інформаційної безпеки відповідальною не може бути лише одна особа. Впровадження цієї політики включає обов'язкове інформування всієї команди та залучених осіб щодо принципів та механізмів дотримання інформації безпеки в організації. Тож кожен працівників чи залучена особа, яка контактує з персональними даними або чутливою інформацію, мають дотримуватися принципів захисту та конфіденційності даних, а також ділити відповідальність у разі витоку даних.

Проте зазвичай в організації має бути визначена особа (група осіб), яка відповідає за впровадження та моніторинг дотримання політики.

Розгляньмо, як може формуватися коло відповідальних за Політику інформаційної безпеки та роботи з персональними даними осіб залежно від розміру неприбуткової організації.

У малій організації (5–10 осіб у команді), яка не має розгалуженої мережі відділів, відповідальною особою може бути керівник або директор. Водночас на рівні відділів відповідальними особами можуть бути спеціаліст, який відповідає за документообіг, наприклад, головний бухгалтер, а також спеціаліст на рівні координації роботи з волонтерами та бенефіціарами, наприклад, проєктний менеджер.

У великих організаціях з розгалуженою мережею відділів та регіональними філіями може бути призначено окрему людину, яка займає посаду чи виконує роль Data Protection Officer (DPO) — фахівця з інформаційної безпеки. У свою чергу, на рівні підрозділів / відділів відповідальними особами можуть бути призначені керівники чи окремі спеціалісти фінансового, проєктного відділів, відділу бухгалтерії, HR-відділу, відділу координації волонтерів тощо. Наповнення цього списку залежить від особливостей структури вашої організації та наявності відділів, які взаємодіють напряму з особистими даними та чутливою інформацію.

Як відрізняються ключові обов'язки головної відповідальної за Політику інформаційної безпеки особи та відповідальних осіб на рівні відділів?

Ключові зобов'язання Data Protection Officer (DPO) або фахівця з інформаційної безпеки:

- Забезпечення дотримання політики на рівні всієї організації.

- Контроль реалізації та моніторинг дотримання політики в організації.

- Забезпечення своєчасного оновлення політики.

- Організація навчання персоналу та залучених осіб щодо дотримання політики в організації.

- Надання консультацій щодо дотримання політики окремим відділам організації.

Ключові зобов'язання відповідальних за дотримання Політики інформаційної безпеки осіб на рівні окремих підрозділів / відділів в організації:

- Дотримання політики у своїй професійній діяльності та контроль реалізації політики у своїй команді.

- Забезпечення надійного зберігання персональних даних та чутливої інформації.

- Оперативне реагування на ризики витоку даних або інциденти.

- Координація процесу надання доступу до даних окремим уповноваженим особам та обмеження доступу серед своєї команди.

5. Консультації з експертами

До розроблення Політики інформаційної безпеки та роботи з персональними даними можна залучати сторонніх спеціалістів, зокрема юристів або правознавців, які спеціалізуються на захисті даних.

Також можуть бути залучені IT-фахівці (або системні адміністратори), які можуть оцінити технічний рівень захисту персональних даних та іншої цифрової інформації, яку зберігає ваша інформація, та впровадити надійні механізми захисту. Також IT-фахівець може допомогти налагодити рівні доступу до даних, механізми шифрування даних, резервного копіювання тощо.

Якщо ви співпрацюєте з донорами, зокрема на міжнародному рівні, варто також проконсультуватися з ними щодо наявності окремих вимог до політики інформаційної безпеки з їхнього боку. Також донори можуть послуговуватися стандартами міжнародного права, власними шаблонами, які варто враховувати під час складання вашої політики.

Якщо ви працюєте напряму з бенефіціарами, в окремих випадках важливо буде проконсультуватися з представником бенефіціарів або групою осіб щодо доступності та зрозумілості запропонованих шаблонів згоди на обробку персональних даних. Для цього також може бути створена фокус-група, яка допоможе проаналізувати потреби бенефіціарів, визначити їхнє ставлення до передачі персональних даних та варіантів їх використання, визначити формат подання інформації в письмовій згоді між бенефіціаром та вашою організацією.

6. Рекомендації щодо заповнення шаблону політики

1. Проаналізуйте запропонований шаблон політики. Визначте, які процеси захисту інформації вже діють у вашій організації (їх потрібно буде лише детально описати в політиці), а які ще потрібно розробити та впровадити з нуля.

2. Перевірте відповідність та універсальність політики. Переконайтеся, що всі її розділи відповідають актуальній структурі й функціонуванню вашої організації та є релевантними для всіх відділів / підрозділів організації. За потреби адаптуйте зміст до особливостей вашої діяльності, типів даних, які обробляються, та технологічних рішень, які використовуються.

3. Переконайтеся, що політика враховує специфіку захисту персональних даних, якими оперує ваша організація. За потреби додайте визначення, процедури або принципи, які охоплюють дані, з якими ви працюєте.

4. Переконайтеся, що визначені терміни, сформовані принципи та процедури спираються на українське законодавство у сфері захисту персональних даних та не суперечать йому.

5. Формулюйте положення політики зрозумілою мовою. Уникайте надміру технічних або юридичних термінів, які можуть ускладнити розуміння. Політика має бути доступною для всіх співробітників організації, зокрема тих, які не мають фахової освіти в ІТ чи юриспруденції.

6. Залучіть фахівців до фінальної перевірки тексту політики. Рекомендовано проконсультуватися з юристом (особливо з фахівцем у сфері захисту персональних даних) та експертами з цифрової безпеки. Також за потреби залучіть працівників, які безпосередньо працюють із вразливими групами бенефіціарів, щоб переконатися, що всі ризики та гарантії враховані.

7. Додайте супровідні документи. Не забудьте в кінці політики розмістити шаблони згоди на обробку персональної інформації та інших документів, якщо такі передбачені.

Заповнення основних розділів політики

Дисклеймер

Цей шаблон є базовою версією Політики інформаційної безпеки та роботи з персональними даними. Вона може не задовольняти вимоги всіх донорів або не охоплювати всі процеси в організації. Її організації можуть використовувати як основу для розроблення власних внутрішніх Політик інформаційної безпеки та роботи з персональними даними.

Залежно від конкретних вимог донорів або внутрішніх потреб організації можуть адаптувати та доопрацьовувати цю політику з огляду на додаткові вимоги та специфікацію своєї діяльності.

Пропонуємо поетапний розгляд окремих розділів шаблону Політики інформаційної безпеки та роботи з персональними даними, який допоможе вам правильно тлумачити її положення та коректно заповнити шаблон.

Під час складання політики важливо в першу чергу орієнтуватися на доступність та зрозумілість мови, яку ви використовуєте, та дати тлумачення всіх понять. Це є надзвичайно важливим для забезпечення однакового трактування змісту політики всіма, хто матиме до неї доступ.

1. Титульна сторінка та зміст

Цей етап заповнення шаблону політики передбачає формулювання її назви, формування місця для її офіційного затвердження в організації, а також визначення основних змістовних розділів, з яких ця політика складатиметься.

Що потрібно в ньому зазначити

- Повну назву вашої організації згідно зі статутом.
- Код неприбутковості та правовий статус організації.
- Інформацію про затвердження політики органами керівництва / правління із вказанням дати затвердження.
- Окреслення розділів, із яких ця політика складається.

На що звернути увагу

- Переконайтеся, що політика буде офіційно затверджена і про це буде вказано на титульній сторінці.
- Перевірте зміст політики, аби він точно відповідав вказаним розділам.

2. Розділи «Сфера застосування» та «Довідкова документація»

Цей розділ розкриває зміст політики, обсяг її дії та вказує на нормативне підґрунтя цього документа.

Що потрібно в ньому зазначити

- Опис меж застосування політики в організації.

- Перелік відповідних законів та міжнародних стандартів, на яких будується ця політика.

На що звернути увагу

- Переконайтеся, що чітко визначено українську законодавчу базу та міжнародні стандарти, на яких базується ваша політика.

- Перевірте, чи зміст політики та використані терміни не суперечать зазначеним нормативним актам та стандартам.

- Оновлюйте за потреби список нормативних актів, на яких базується політика, щоб вона відповідала актуальним вимогам.

3. Розділ «Терміни та їхні визначення»

Цей розділ містить перелік специфічних термінів, що використовуються в політиці, і їхні визначення для забезпечення чіткого розуміння та однакового трактування всіма учасниками процесу.

Що потрібно в ньому зазначити

- Список усіх термінів, що використовуються в політиці (наприклад, «персональні дані», «інформація» тощо).

- Визначення кожного терміна для уникнення двозначного трактування.

На що звернути увагу

- Переконайтеся, що визначення є точними та відповідають чинному законодавству, нормативним актам та міжнародним стандартам.

4. Розділ «Політика Інформаційної безпеки»

Цей розділ визначає загальні цілі та основні завдання організації щодо захисту інформації та персональних даних, які в подальшому будуть розкриті в цій політиці.

Що потрібно в ньому зазначити

- Головні цілі політики інформаційної безпеки та роботи з персональними даними.

- Завдання, реалізацію яких має забезпечити ця політика.

На що звернути увагу

- Підкресліть відповідність політики вимогам законодавства та (за потреби) вимогам міжнародних нормативних актів.

- Зазначте лише ті завдання, які будуть в повній мірі розкриті в цій політиці і які ця політика здатна регулювати.

5. Розділ «Отримання згоди на обробку персональних даних»

Цей розділ окреслює підґрунтя для отримання згоди на обробку персональних даних та визначає перелік осіб, у яких може бути взята відповідна згода, та, найважливіше, він містить перелік інформації, яка визначається персональними даними згідно із законодавством України. Також він описує процес отримання згоди суб'єкта даних на обробку його персональних даних відповідно до законодавства.

Що потрібно в ньому зазначити

- Визначення усіх учасників процесу, з якими взаємодіє ваша організація та чиї дані можуть бути використані організацією за відповідної згоди.

- Розкриття поняття «персональні дані» та визначення переліку інформації, яку охоплює це поняття.

- Основний зміст та характеристики згоди на обробку персональних даних.

- Процедуру отримання згоди на обробку персональних даних.

- Визначення принципів отримання такої згоди.

- Опис умов, за яких можна припинити обробку даних та відкликати згоду.

На що звернути увагу

- Переконайтеся, що вказані терміни та їхні визначення базуються на Законі України «Про захист персональних даних».

- Перевірте, чи описані характеристики та зміст згоди відповідають шаблону такої згоди, що має міститься в додатках до цієї політики.

6. Розділ «Управління базами даних, які містять інформацію про персональні дані»

Цей розділ визначає, як здійснюється управління базами даних, що містять персональні дані, з метою їх захисту та правильного використання.

Що потрібно в ньому зазначити

- Процес збереження персональних даних у вигляді баз даних.

- Шаблон бази даних, що має використовуватися організацією для збору персональних даних.

- Окреслення вимог щодо обов’язкового ознайомлення з політикою всіх працівників та залучених осіб.

- Окреслення сфер діяльності організації, які вимагають збору та обробки персональних даних.

На що звернути увагу

- Перевірте, що сформовані бази даних у вашій організації відповідають шаблону, наведеному в політиці.

- Переконайтеся, що всі бази даних, які зберігаються у вашій організації, є уніфікованими та мають однакові розділи.

- Упевніться, що всі працівники та залучені особи ознайомлені з політикою та підписали відповідні документи про ознайомлення.

7. Розділ «Дії у випадку виявлення витоку персональних даних»

Цей розділ визначає алгоритм дій у разі виявлення витоку персональних даних з метою мінімізації ризиків, інформування постраждалих та запобігання подібним інцидентам у майбутньому.

Що потрібно в ньому зазначити

- Процедуру оцінювання ситуації після виявлення витоку персональних даних.

- Негайні дії, спрямовані на обмеження доступу, усунення причин витоку персональних даних та залучення відповідних фахівців у разі підозри на злочинні дії.

- Алгоритм інформування відповідних органів.

- Інформацію про процес інформування осіб, чиї дані були скомпрометовані, з рекомендаціями щодо захисту.

- Кроки, які необхідно зробити в межах внутрішнього розслідування та оновлення політики безпеки.

- Дії для залагодження інцидентів з юридичної та репутаційної точок зору.

На що звернути увагу

- Дії мають бути вжиті негайно після виявлення витоку персональних даних — що раніше, то менше ризиків виникне.

- Оцінювання масштабу витоку персональних даних повинне бути детальним і містити класифікацію даних, що потрапили в сторонні руки.

- Після інциденту слід провести навчання персоналу з питань інформаційної безпеки, щоб запобігти повторенню ситуації.

8. Розділ «Механізм надання інформації та персональних даних третім особам»

Цей розділ визначає правила, умови та обмеження щодо передачі персональних даних третім особам згідно з чинним законодавством України та міжнародними нормами, а також описує порядок дій у випадках дозволеної чи забороненої передачі даних.

Що потрібно в ньому зазначити

- Визначення загальних принципів передачі персональних даних.

- Чітке розмежування та визначення ситуацій, у яких передача даних дозволена, і випадків, коли передача заборонена.

- Алгоритм дій на випадок дозволеної передачі даних та порядок дій у випадку, якщо передача даних заборонена.

На що звернути увагу

- Передача даних має здійснюватися в межах правового поля та спиратися на законодавство України, зокрема на Закон «Про захист персональних даних».

- Згода має бути зрозумілою, а всі особи, чиї дані передаються, особливо з-поміж вразливих верств населення, повинні бути поінформовані.

9. Розділ «Відповідальність»

Цей розділ описує, хто несе відповідальність за впровадження та моніторинг дотримання Політики інформаційної безпеки та роботи з персональними даними в організації.

Що потрібно в ньому зазначити

- Визначення осіб, відповідальних за розроблення передбачених політикою процедур.

- Призначення особи (групи осіб), відповідальної за дотримання політики в організації.

На що звернути увагу

- Призначайте відповідальних осіб відповідно до розміру вашої організації та розгалуженості мережі відділів. За потреби призначте головну відповідальну особу та відповідальних на рівні відділів / підрозділів організації.

- За потреби складіть перелік ключових обов'язків відповідальних осіб.

10. Шаблони документів

Цей розділ містить шаблони документів, які використовуються для забезпечення виконання політики.

Що потрібно в ньому зазначити

- Шаблони згоди на отримання згоди на обробку персональних даних.

- Інші шаблони, які регулюватимуть дотримання політики та використовуватимуться в організації (наприклад, шаблон звітності щодо витоку даних).

На що звернути увагу

- Переконайтеся, що шаблони відповідають вимогам законодавства.

- Перевірте, чи шаблони, розміщені в політиці, відповідають шаблонам документів, які ваша організація використовує на практиці.

- За потреби розробіть кілька варіантів шаблонів згоди на обробку персональних даних залежно від цільової аудиторії. Це важливо для того, щоб забезпечити повне розуміння змісту угоди всіма цільовими групами.

Наступні кроки після заповнення шаблону політики

- **Перевірка відповідності політики фактичним процесам.**

Перегляньте зміст політики на відповідність реальним процесам обробки та зберігання даних, які використовуються в організації. Переконайтеся, що описані заходи справді відповідають наявним практикам безпеки.

- **Аналіз покриття всіх ключових аспектів інформаційної безпеки.**

Перевірте, чи зміст політики охоплює всі можливі аспекти захисту персональних даних та процедури реагування в ситуаціях їх витоку.

- **Узгодження з вимогами партнерів і донорів.**

Звірте політику з вимогами зовнішніх партнерів, донорських організацій або наглядових органів, якщо організація з ними співпрацює. За потреби адаптуйте документ під їхні стандарти.

- **Підготовка політики до затвердження.**

Підготуйте фінальну версію документа для розгляду керівництвом (директором, правлінням, наглядовою радою тощо). Додайте титульну сторінку, на якій буде вказано рішення про затвердження, дату, підпис відповідальної особи.

- **Офіційне ухвалення політики.**

Організуйте процес затвердження політики: голосування, підписання рішення або протоколу на засіданні. Зафіксуйте ухвалення політики в офіційних документах.

- **Ознайомлення всіх залучених сторін.**

Поширте затверджену політику серед працівників, підрядників, волонтерів, партнерів та всіх інших залучених сторін. Організуйте процес ознайомлення з політикою та процедуру **обов'язкового письмового підтвердження факту ознайомлення.**

- **Забезпечення доступності документа.**

Розмістіть політику у внутрішньому середовищі організації, щоб в усіх залучених сторін за потреби був до неї доступ.

- **Проведення навчання персоналу.**

Організуйте тренінги чи інформаційні сесії щодо політики для персоналу організації, а також (за потреби) для волонтерів чи інших залучених сторін.

- **Підготовка пояснювальних матеріалів.**

Розробіть зручні для сприйняття інструменти для ознайомлення та навчання: інфографіку, FAQ, коротку презентацію із основними положеннями політики тощо.

- **Інтеграція політики в щоденну діяльність.**

Переконайтеся, що політика не є формальністю та включена в посадові інструкції співробітників, застосовується в роботі з бенефіціарами.

- **Встановлення періодичності перегляду.**

Пропишіть, як часто буде здійснюватися перегляд та оновлення політики (наприклад, раз на рік або після інцидентів). Визначте оновлення політики як одне із завдань відповідальної за політику особи.

Відповіді на найбільш поширені запитання

1. Як зрозуміти, яка інформація є чутливою або особистою, а яку ми можемо використовувати публічно без згоди?

Визначення та зміст особистої (персональної) інформації містяться та регулюються Законом України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року. Згідно з визначенням у цьому законі, персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Визначення чутливої інформації немає в цьому законі, проте його стаття 7 визначає особливі вимоги до обробки персональних даних. Ми можемо стверджувати, що ці особливі вимоги стосуються якраз чутливої, особливої інформації. Це інформація про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також дані, що стосуються здоров'я, статевого життя, біометричні або генетичні дані.

Такі дані не можна передавати або публікувати без прямої згоди особи. Без згоди можна використовувати лише анонімну, статистичну або відкриту згідно із законом інформацію, яка не дає змоги ідентифікувати конкретну особу.

2. Чи можна використовувати кейси бенефіціарів у публічних звітах або на сайті організації?

Кейси бенефіціарів з описом ситуації, розкриттям особистих даних чи використанням фотографій можна використовувати лише за умови надання ними письмової згоди. Пам'ятайте, що якщо йдеться про дітей або дорослих, які не здатні надати згоду особисто, публікації мають бути узгоджені із їхнім законним опікуном.

3. Що робити, якщо партнерська або донорська організація просить поділитися базою бенефіціарів, що містить персональні дані осіб?

Ви не можете передавати персональні дані третім особам без відповідної письмової згоди бенефіціарів. Переконайтеся, що у вас є згоди всіх уміщених у базі бенефіціарів, перш ніж її передавати.

4. Що робити з більше не потрібними паперовими документами, які містять персональні дані бенефіціарів?

Ми не рекомендуємо одразу після завершення проєктів позбавлятися всієї інформації, яка їх стосується. Ця інформація може знадобиться у випадках складання звітності, річного звітування, проведення аудиту, моніторингу довготривалого ефекту від проєкту тощо.

Проте якщо у вас є потреба знищити архівні документи, які містять персональні дані, переконайтеся, що це знищення відбувається в безпечний спосіб. Папери з персональними даними не можна просто викидати — обов'язково використовуйте шредер.

5. Чи можуть бенефіціари вимагати видалення своїх даних?

Звичайно, бенефіціари або будь-які інші особи, які надали згоду на обробку персональних даних вашій організації, мають право в будь-який момент відкликати надану згоду. Тож організація буде змушена в цьому випадку видалити ці дані там, де вони були розміщені, а також знищити в безпечний спосіб ці дані з архівів організації.