ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ

інформаційно-аналітичної системи «Perevir»

Дата набрання чинності: [01.09.2019 року]
Дата останнього оновлення: [28 квітня 2026 року]

1. Загальні положення та сфера застосування

1.1. Ця Політика конфіденційності інформаційно-аналітичної системи «Perevir» (далі - **Політика**) визначає порядок збирання, отримання, реєстрації, накопичення, зберігання, використання, структурування, зіставлення, передавання, захисту, знеособлення, обмеження, видалення та іншої обробки персональних даних у зв'язку з функціонуванням і використанням інформаційно-аналітичної системи «Perevir».

1.2. Політика поширюється на інформаційно-аналітичну систему «Perevir», її вебсайт, особистий кабінет, програмний інтерфейс, мобільні або вебзастосунки, API, модулі, інтеграції, сервіси моніторингу, електронної ідентифікації та інші пов'язані функціональні можливості, якщо для них не встановлена окрема політика конфіденційності.

1.3. Perevir є інформаційно-аналітичною системою, призначеною, зокрема, для:

- пошуку інформації про юридичних осіб, фізичних осіб - підприємців та інших суб'єктів;
- отримання та відображення інформації з державних, офіційних, відкритих, договірних та інших законних джерел;
- структурування й зіставлення інформації;
- формування інформаційних та аналітичних звітів;
- перевірки контрагентів;
- оцінювання правових, фінансових, санкційних, репутаційних та інших ризиків;
- налаштування моніторингу суб'єктів;
- надсилання повідомлень про зміни;
- надання інших інформаційно-аналітичних функцій.

1.4.Ця Політика застосовується до персональних даних:

1. осіб, які відвідують вебсайт Perevir;
2. осіб, які створюють або використовують обліковий запис Perevir;
3. уповноважених представників юридичних осіб та інших корпоративних Користувачів;
4. осіб, які проходять електронну ідентифікацію або автентифікацію;

5. осіб, які звертаються до служби підтримки, надсилають запити, заяви, скарги або інші повідомлення;
6. осіб, дані про яких містяться в державних реєстрах, відкритих даних, офіційних джерелах або інших законно отриманих інформаційних ресурсах;
7. інших фізичних осіб, персональні дані яких обробляються під час використання Perevir.

1.5.Політика регулює обробку двох основних категорій інформації:

- **персональних даних Користувачів Perevir**, які збираються під час реєстрації, ідентифікації, використання облікового запису, оплати, звернення до служби підтримки та взаємодії із Системою;
- **персональних даних третіх осіб**, які можуть міститися в державних реєстрах, відкритих даних, судових рішеннях, офіційних інформаційних ресурсах, комерційних базах даних або інших законних джерелах.

1.6. Perevir не є первинним джерелом більшості відомостей про третіх осіб, які відображаються в інформаційних та аналітичних звітах.

Система може здійснювати технічний пошук, отримання, структурування, зіставлення, систематизацію, візуалізацію та аналітичне опрацювання відповідної інформації без самостійного внесення змін до її змісту в первинному джерелі.

1.7.Ця Політика застосовується незалежно від способу доступу до Perevir, зокрема через:

- веббраузер;
- особистий кабінет;
- мобільний пристрій;
- API;
- інтеграцію з іншою інформаційною системою;
- корпоративний обліковий запис;
- інший технічно доступний канал.

1.8.Обробка персональних даних здійснюється відповідно до:

- Конституції України;
- Закону України «Про захист персональних даних»;
- Закону України «Про інформацію»;
- Закону України «Про доступ до публічної інформації»;
- Закону України «Про електронні документи та електронний документообіг»;
- Закону України «Про електронну ідентифікацію та електронні довірчі послуги»;
- інших застосовних нормативно-правових актів України;
- Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 - GDPR, якщо він застосовується до конкретної операції обробки.

1.9.Ця Політика є складовою правової документації Perevir та застосовується разом із:

- Правилами користування Perevir;
- договором про обробку персональних даних, якщо він укладається;
- Політикою використання cookies;
- іншими документами, на які міститься посилання в Системі або договорі.

1.10.У разі суперечності між цією Політикою та окремим письмовим договором щодо обробки персональних даних перевагу мають положення такого договору, якщо інше не передбачено імперативними нормами законодавства.

1.11.Використання Perevir означає, що Користувач ознайомився з цією Політикою. У випадках, коли законодавство вимагає окремої згоди на обробку персональних даних, така згода отримується окремо і не замінюється самим фактом ознайомлення з Політикою.

1.12.Надання згоди не є єдиною правовою підставою обробки персональних даних у Perevir.

Залежно від конкретної операції обробка може здійснюватися на підставі:

- виконання договору;
- вчинення дій до укладення договору;
- виконання обов’язку, встановленого законом;
- законного інтересу;
- дозволу на обробку даних, наданого законом;
- необхідності встановлення, реалізації або захисту правових вимог;
- згоди суб’єкта персональних даних;
- іншої правової підстави, передбаченої законодавством.

1.13.Політика не визначає правила використання інформації Користувачем після її отримання через Perevir. Користувач самостійно відповідає за законність подальшого використання, зберігання, передавання, поширення та іншої обробки отриманої інформації відповідно до Правил користування Perevir і застосовного законодавства.

1.14. Політика не поширюється на вебсайти, інформаційні системи та сервіси третіх осіб, навіть якщо посилання на них або доступ до них надається через Perevir. Обробка інформації такими особами регулюється їхніми власними політиками та умовами.

1.15.Якщо Користувач діє від імені юридичної особи, він підтверджує наявність повноважень на:

- використання Perevir від імені такої юридичної особи;
- передавання персональних даних її працівників або представників;
- прийняття цієї Політики та інших умов використання;

- надання необхідних інструкцій щодо обробки персональних даних.

1.16.Якщо Користувач передає до Perevir персональні дані інших осіб, він підтверджує, що:

- має належну правову підставу для такого передавання;
- визначив законну та конкретну мету обробки;
- належним чином поінформував відповідних суб'єктів даних, якщо це вимагається законодавством;
- не передає надмірних або не пов'язаних із метою використання даних;
- не використовує Perevir для незаконного збирання, профілювання, переслідування або дискримінації осіб.

2. Терміни та визначення

2.1.У цій Політиці наведені нижче терміни вживаються в такому значенні.

2.2. Адміністрація Perevir, Адміністрація, ми, нас, наш

ТОВ «БІНОТЕЛ АЙТІ - СЕРВІС», яка забезпечує функціонування Perevir, визначає умови надання доступу до Системи та в передбачених цією Політикою випадках здійснює обробку персональних даних.

2.3. Perevir, Система

Інформаційно-аналітична система «Perevir», включаючи вебсайт, особистий кабінет, програмне забезпечення, бази даних, модулі, API, інтеграції, сервіси моніторингу та інші функціональні компоненти.

2.4. Користувач

Фізична особа, фізична особа - підприємець, представник юридичної особи або інша особа, яка відвідує вебсайт, реєструється, проходить ідентифікацію, використовує Perevir або взаємодіє з Адміністрацією.

2.5. Корпоративний Користувач

Юридична особа, фізична особа - підприємець або інший суб'єкт, який уклав договір щодо використання Perevir і надає доступ до Системи своїм працівникам, представникам або іншим уповноваженим особам.

2.6. Суб'єкт персональних даних

Фізична особа, яка ідентифікована або може бути конкретно ідентифікована та якої стосуються персональні дані.

2.7. Персональні дані

Відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути прямо чи опосередковано ідентифікована.

2.8. Дані Користувача

Персональні дані, технічні відомості та інша інформація, що стосуються Користувача і збираються або створюються під час реєстрації, автентифікації, електронної ідентифікації та використання Perevir.

2.9. Реєстрові дані

Інформація, отримана з державних реєстрів, офіційних інформаційних ресурсів, відкритих наборів даних, судових ресурсів, систем публічних закупівель та інших законних джерел.

2.10. Дані третіх осіб

Персональні дані фізичних осіб, які не є Користувачами Perevir, але відомості про яких можуть міститися у реєстрових даних, документах, запитах Користувача або інших джерелах інформації.

2.11. Обробка персональних даних

Будь-яка дія або сукупність дій, здійснених повністю або частково в інформаційній системі чи в інший спосіб, пов’язаних зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням, структуруванням, зіставленням, передаванням, поширенням, знеособленням, обмеженням, видаленням або знищенням персональних даних.

2.12. Володілець персональних даних

Фізична або юридична особа, яка визначає мету обробки персональних даних, склад цих даних і процедури їх обробки, якщо інше не визначено законом.

Для цілей GDPR термін за змістом відповідає поняттю **контролер персональних даних**.

2.13. Розпорядник персональних даних

Фізична або юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

Для цілей GDPR термін за змістом відповідає поняттю **обробник персональних даних**.

2.14. Контролер персональних даних, Controller

Особа, яка самостійно або спільно з іншими особами визначає цілі та засоби обробки персональних даних у розумінні GDPR.

2.15. Обробник персональних даних, Processor

Особа, яка обробляє персональні дані від імені та за документованими вказівками контролера у розумінні GDPR.

2.16. Спільні контролери

Дві або більше осіб, які спільно визначають цілі та істотні засоби конкретної операції обробки персональних даних.

2.17. Одержувач

Особа, якій розкриваються або передаються персональні дані, незалежно від того, чи є вона третьою особою.

2.18. Третя особа

Будь-яка особа, крім суб'єкта персональних даних, володільця, розпорядника, контролера, обробника та осіб, які безпосередньо уповноважені обробляти дані під їхнім керівництвом.

2.19. Постачальник послуг, субпроцесор

Третя особа, яка залучається Адміністрацією для забезпечення хостингу, зберігання, аналітики, підтримки, комунікацій, інформаційної безпеки, ідентифікації, оплати або іншої функціональності Perevir.

2.20. Обліковий запис

Сукупність даних і технічних засобів, за допомогою яких Користувач отримує персоналізований доступ до Perevir.

2.21. Автентифікація

Електронний процес перевірки належності Користувачу даних доступу, облікового запису або засобу електронної ідентифікації.

2.22. Електронна ідентифікація

Процес використання персональних ідентифікаційних даних в електронній формі для однозначного визначення фізичної, юридичної особи або її представника.

2.23. Кваліфікований електронний підпис, КЕП

Удосконалений електронний підпис, створений із використанням засобу кваліфікованого електронного підпису та заснований на кваліфікованому сертифікаті відкритого ключа.

2.24. Дія.Підпис

Засіб електронної ідентифікації та електронного підпису, що використовується через відповідні державні інформаційні системи та застосунок «Дія».

2.25. РНОКПП

Реєстраційний номер облікової картки платника податків, який може використовуватися для електронної ідентифікації та забезпечення законного доступу до окремої інформації.

2.26. API

Програмний інтерфейс, за допомогою якого інформаційні системи можуть автоматизовано обмінюватися даними та функціональними командами.

2.27. Cookies

Невеликі текстові файли або інші ідентифікатори, які зберігаються на пристрої Користувача або зчитуються з нього під час використання вебсайту чи Системи.

2.28. Технічні дані

Інформація про пристрій, браузер, операційну систему, IP-адресу, сесію, часові мітки, дії в Системі, журнали подій та інші технічні параметри використання Perevir.

2.29. Логування

Автоматизована фіксація технічних, операційних і безпекових подій, що виникають під час використання Perevir.

2.30. Профілювання

Автоматизована обробка персональних даних для оцінювання або прогнозування окремих характеристик фізичної особи, зокрема її поведінки, інтересів, надійності чи ризиків.

2.31. Автоматизоване рішення

Рішення, яке приймається виключно на підставі автоматизованої обробки персональних даних без змістовної участі людини та створює юридичні або подібні істотні наслідки для фізичної особи.

2.32. Знеособлення

Обробка персональних даних у спосіб, після якого визначення фізичної особи неможливе або вимагає непропорційних витрат часу, ресурсів чи засобів.

2.33. Псевдонімізація

Обробка персональних даних у спосіб, за якого вони без використання додаткової інформації не можуть бути віднесені до конкретної фізичної особи, за умови окремого зберігання та захисту такої додаткової інформації.

2.34. Порушення безпеки персональних даних

Подія, що призвела або могла призвести до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття персональних даних або доступу до них.

2.35. GDPR

Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних.

2.36.

Інші терміни вживаються у значеннях, визначених законодавством України, GDPR, Правилами користування Perevir та відповідними договорами.

3. Володілець персональних даних

3.1.Володільцем персональних даних Користувачів Perevir є:

ТОВ «БІНОТЕЛ АЙТІ - СЕРВІС»

Юридична адреса:
м. Київ, 02081, вул. Здолбунівська 7Д корпус 3,Бізнес-центр "Аполло", 2 поверх.

Контактні дані для загальних питань та звернень щодо використання Perevir:

Електронна пошта:
support@perevir.ua

Телефон:
+38 044 344 04 44

+38 067 344 04 44 (багатоканальний)
+38 050 344 04 44 (багатоканальний)
+38 093 344 04 44 (багатоканальний)

Далі в цій Політиці - **Адміністрація Perevir**, **Адміністрація**, **ми**, **нас** або **наш**.

3.2.Адміністрація виступає володільцем персональних даних, а за наявності підстав для застосування GDPR - контролером персональних даних, коли вона самостійно визначає мету та істотні засоби обробки.

3.3.Адміністрація є володільцем або контролером, зокрема, щодо обробки:

- даних реєстрації Користувача;
- даних облікового запису;
- електронної адреси;
- номера телефону;
- ПІБ;
- даних представника корпоративного Користувача;
- даних електронної ідентифікації;
- РНОКПП, якщо він обробляється для належної ідентифікації та доступу;
- технічних даних;
- IP-адреси;
- даних про сесії;
- журналів доступу;
- історії операцій у Системі;
- даних тарифного плану та розрахунків;
- звернень до служби підтримки;
- налаштувань моніторингу;
- інформації, необхідної для захисту Системи, запобігання шахрайству та виконання законодавчих обов’язків.

3.4.Адміністрація самостійно визначає цілі та засоби обробки зазначених даних, зокрема для:

- створення й адміністрування облікового запису;
- надання доступу до Perevir;
- автентифікації та електронної ідентифікації;
- виконання договору;
- надання інформаційно-аналітичних функцій;
- забезпечення роботи моніторингу;
- комунікації з Користувачем;
- виставлення рахунків та обліку платежів;

- забезпечення інформаційної безпеки;
- журналювання та аудиту;
- запобігання зловживанням;
- удосконалення функціональності;
- виконання законодавчих та регуляторних вимог;
- встановлення, реалізації та захисту правових вимог.

3.5.Стосовно персональних даних третіх осіб, отриманих із державних реєстрів, офіційних ресурсів, відкритих даних та інших зовнішніх джерел, роль Адміністрації визначається залежно від:

- джерела інформації;
- правової підстави доступу;
- характеру операції;
- мети використання інформації;
- змісту договору з постачальником даних;
- ступеня самостійності Адміністрації у визначенні цілей та засобів обробки.

3.6.Сам факт технічного відображення або передавання відомостей із зовнішнього джерела не означає, що Адміністрація є первинним володільцем відповідного державного реєстру або автором відомостей, які містяться в ньому.

Первинним володільцем, держателем, адміністратором або розпорядником відповідного джерела може бути державний орган, державне підприємство, суд, орган місцевого самоврядування, комерційний постачальник або інша визначена законом особа.

3.7.Адміністрація може виступати самостійним володільцем або контролером щодо похідної обробки інформації, якщо вона самостійно визначає цілі та засоби:

- структурування даних;
- об’єднання відомостей із декількох джерел;
- формування звітів;
- створення графів зв’язків;
- визначення технічних збігів;
- формування аналітичних показників;
- створення індикаторів ризику;
- ведення журналів запитів;
- організації моніторингу змін.

3.8.Якщо корпоративний Користувач самостійно визначає:

- осіб, щодо яких здійснюється перевірка;
- мету перевірки;
- категорії даних;

- критерії пошуку;
- строк зберігання результатів;
- порядок використання та передавання результатів,

такий корпоративний Користувач може виступати окремим володільцем або контролером персональних даних у межах своєї діяльності.

3.9.У випадку, передбаченому пунктом 3.8 цієї Політики, Адміністрація може виступати розпорядником або обробником персональних даних у частині операцій, які вона виконує виключно від імені та за документованими вказівками корпоративного Користувача.

Такі відносини можуть додатково регулюватися договором про обробку персональних даних.

3.10.Корпоративний Користувач несе відповідальність за:

- наявність правової підстави обробки;
- законність мети перевірки;
- інформування суб'єктів даних, якщо це необхідно;
- дотримання принципу мінімізації;
- встановлення належного строку зберігання;
- виконання запитів суб'єктів персональних даних;
- законність використання результатів Perevir;
- недопущення дискримінаційних або незаконних рішень.

3.11.Адміністрація не вважається розпорядником або обробником лише через те, що Користувач використовує загальнодоступну функціональність Perevir на власний розсуд.

Для виникнення відносин «володілець - розпорядник» або «контролер - обробник» повинні бути наявні документовані вказівки, відповідний розподіл ролей і, за необхідності, окремий договір.

3.12.Адміністрація може залучати інших розпорядників, обробників або субпроцесорів для забезпечення роботи Perevir, зокрема постачальників:

- хмарної інфраструктури;
- хостингу;
- резервного копіювання;
- електронної пошти;
- технічної підтримки;
- аналітики;
- моніторингу;
- інформаційної безпеки;

- електронної ідентифікації;
- платіжних послуг;
- API та інформаційних даних.

3.13.Залучені постачальники отримують доступ до персональних даних лише в обсязі, необхідному для виконання відповідних функцій, та повинні дотримуватися договірних, законодавчих і безпекових вимог щодо захисту інформації.

3.14.Якщо цілі та засоби певної обробки визначаються Адміністрацією спільно з іншою особою, сторони можуть виступати спільними контролерами.

У такому разі розподіл їхніх обов'язків може встановлюватися окремою угодою або законодавством.

3.15.Контактним підрозділом із питань захисту персональних даних є:

Електронна пошта:
privacy@binotel.com

3.16.Зазначення контактного підрозділу не означає автоматичного призначення формального уповноваженого із захисту даних - Data Protection Officer, якщо обов'язок такого призначення не виникає відповідно до GDPR або іншого застосовного законодавства.

3.17.Інформація про конкретну роль Адміністрації у певній операції обробки може додатково визначатися:

- цією Політикою;
- договором із Користувачем;
- договором про обробку персональних даних;
- повідомленням під час збирання даних;
- умовами конкретної функції Perevir;
- законодавством;
- правилами відповідного державного чи комерційного джерела.

4. Хто відповідає за обробку персональних даних

4.1.Відповідальність за обробку персональних даних у межах функціонування Perevir розподіляється залежно від того:

- хто визначає мету обробки;
- хто визначає склад персональних даних;
- хто встановлює способи та строки їх обробки;
- від чийого імені здійснюється відповідна операція;
- з якого джерела отримані дані;

- на якій правовій підставі здійснюється обробка.

4.2.Адміністрація Perevir відповідає за обробку персональних даних, щодо яких вона самостійно визначає мету, обсяг і способи обробки.

До таких даних, зокрема, можуть належати:

- реєстраційні дані Користувача;
- дані облікового запису;
- контактні дані;
- дані електронної ідентифікації;
- технічні дані;
- журнали входів і дій у Системі;
- інформація про тарифний план та оплату;
- звернення до служби підтримки;
- налаштування Користувача;
- дані, необхідні для забезпечення безпеки, запобігання шахрайству та виконання вимог законодавства.

Наявна політика Perevir уже передбачає обробку реєстраційних, ідентифікаційних і технічних даних, зокрема електронної пошти, ПІБ, РНОКПП, IP-адреси, cookies та інформації про сесії.

4.3.Адміністрація відповідає за забезпечення належної організації обробки персональних даних, зокрема за:

- визначення законної та конкретної мети обробки;
- визначення правової підстави;
- дотримання принципу мінімізації даних;
- обмеження строків зберігання;
- забезпечення точності даних у межах власної сфери контролю;
- встановлення правил доступу;
- застосування технічних та організаційних заходів безпеки;
- ведення журналів подій;
- реагування на інциденти;
- розгляд звернень суб’єктів персональних даних;
- залучення постачальників із належними гарантіями захисту даних.

4.4.Адміністрація не є первинним держателем, адміністратором або автором інформації, отриманої з державних реєстрів, офіційних ресурсів, судових систем, відкритих даних або інших зовнішніх джерел.

Відповідальність за ведення відповідного реєстру, первинне внесення, оновлення та достовірність відомостей несе визначений законодавством держатель, адміністратор, розпорядник або інший уповноважений суб’єкт.

4.5.Адміністрація відповідає за ті операції з інформацією із зовнішніх джерел, які здійснюються безпосередньо в Perevir, зокрема за:

- законність способу отримання даних;
- дотримання встановлених обмежень доступу;
- захист інформації під час передавання та зберігання;
- структурування і технічне відображення;
- обмеження доступу відповідно до ролі Користувача;
- журналювання запитів;
- формування похідних аналітичних матеріалів;
- видалення або обмеження обробки у випадках, передбачених законом.

4.6. Perevir не несе відповідальності за помилки, застарілі, неповні або суперечливі відомості, якщо вони були отримані з первинного зовнішнього джерела без зміни їхнього змісту Системою.

У разі розбіжностей юридично значущу інформацію необхідно перевіряти безпосередньо у відповідному офіційному джерелі.

4.7.Корпоративний Користувач відповідає за обробку персональних даних, якщо він самостійно визначає:

- кого саме перевіряти;
- з якою метою проводиться перевірка;
- які критерії пошуку використовуються;
- як застосовуватимуться результати;
- кому вони передаватимуться;
- протягом якого строку вони зберігатимуться;
- які рішення прийматимуться на їх підставі.

4.8.Корпоративний Користувач зобов’язаний забезпечити:

- наявність належної правової підстави для перевірки;
- законність мети;
- пропорційність обсягу даних;
- дотримання прав суб’єктів персональних даних;
- недопущення незаконної дискримінації;
- недопущення використання даних для переслідування, шантажу, спаму або інших неправомірних цілей;
- належний захист отриманих через Perevir результатів.

4.9.Якщо Користувач передає до Perevir персональні дані інших фізичних осіб, він відповідає за:

- законність такого передавання;

- достовірність наданої інформації;
- наявність відповідної правової підстави;
- інформування суб’єктів даних, якщо це вимагається законом;
- дотримання принципу мінімізації;
- виконання інших обов’язків володільця або контролера даних.

4.10.Постачальники послуг, які залучаються Адміністрацією, відповідають за належне виконання покладених на них операцій у межах договорів, законодавства та документованих інструкцій Адміністрації.

До таких постачальників можуть належати:

- провайдери хостингу;
- хмарні постачальники;
- сервіси резервного копіювання;
- засоби електронної ідентифікації;
- платіжні сервіси;
- системи аналітики;
- сервіси моніторингу;
- постачальники інформаційної безпеки;
- оператори електронних комунікацій;
- постачальники API та інформаційних даних.

Загальна політика Binotel також передбачає залучення сторонніх постачальників для аналітики, моніторингу безпеки, доступності та хмарного зберігання з вимогою належного рівня захисту даних.

4.11.Працівники, підрядники та інші уповноважені особи Адміністрації можуть обробляти персональні дані лише:

- у межах наданих їм повноважень;
- для виконання службових або договірних обов’язків;
- відповідно до внутрішніх політик;
- за принципом найменших привілеїв;
- із дотриманням конфіденційності та вимог інформаційної безпеки.

4.12.Доступ працівників і підрядників до персональних даних може журналюватися, контролюватися та періодично переглядатися.

4.13.Адміністрація може призначити відповідальну особу, підрозділ або комітет з питань захисту персональних даних та інформаційної безпеки.

Контактні дані відповідальної особи або підрозділу зазначаються у розділі «Контактна інформація» цієї Політики.

4.14.Призначення внутрішньої відповідальної особи або підрозділу не означає автоматичного призначення формального Data Protection Officer відповідно до статті 37 GDPR, якщо обов'язок такого призначення не виникає згідно із застосовним законодавством.

4.15.Якщо запит суб'єкта персональних даних стосується інформації, щодо якої корпоративний Користувач є самостійним володільцем або контролером, Адміністрація може:

- направити заявника до відповідного корпоративного Користувача;
- передати запит корпоративному Користувачу;
- надати йому технічне сприяння;
- виконати операцію за його документованою вказівкою, якщо це передбачено договором.

4.16.Розподіл відповідальності може додатково визначатися:

- договором про надання послуг;
- договором про обробку персональних даних;
- умовами конкретного тарифного плану;
- правилами використання API;
- умовами відповідної інтеграції;
- вимогами державного реєстру або зовнішнього постачальника;
- законодавством України та, якщо застосовується, GDPR.

5. Ролі Perevir під час обробки даних

5.1.Під час обробки персональних даних Perevir може виконувати різні правові та функціональні ролі залежно від характеру конкретної операції.

Роль Perevir визначається не назвою послуги або договору, а тим, хто фактично визначає мету та істотні засоби обробки персональних даних.

5.2. Perevir як володілець або контролер персональних даних

Perevir виступає володільцем персональних даних у розумінні законодавства України, а за умови застосування GDPR — контролером, якщо Адміністрація самостійно визначає мету та способи обробки.

5.3. Perevir виступає володільцем або контролером, зокрема, під час:

- реєстрації Користувача;
- створення та адміністрування облікового запису;

- автентифікації;
- електронної ідентифікації;
- обробки контактних даних;
- ведення історії входів і сесій;
- обробки технічних журналів;
- забезпечення інформаційної безпеки;
- запобігання шахрайству та зловживанням;
- виставлення рахунків;
- комунікації з Користувачем;
- розгляду звернень;
- адміністрування тарифів;
- аналітики використання Системи;
- удосконалення Perevir;
- виконання юридичних та регуляторних обов'язків.

5.4.У цій ролі Perevir самостійно відповідає за:

- визначення правової підстави;
- прозоре інформування суб'єктів даних;
- дотримання прав суб'єктів;
- визначення строків зберігання;
- вибір постачальників;
- установлення заходів безпеки;
- документування операцій обробки;
- реагування на порушення безпеки.

5.5. Perevir як розпорядник або обробник персональних даних

Perevir може виступати розпорядником у розумінні законодавства України або обробником у розумінні GDPR, якщо обробляє персональні дані:

- від імені корпоративного Користувача;
- за його документованими вказівками;
- для визначеної ним мети;
- у межах укладеного договору;
- без самостійного використання таких даних для несумісних цілей.

5.6. Perevir може виконувати роль обробника, зокрема, коли корпоративний Користувач:

- завантажує власні списки осіб або контрагентів;
- налаштовує перевірку визначених ним осіб;
- створює внутрішні списки моніторингу;
- зберігає результати перевірок у корпоративному кабінеті;
- інтегрує Perevir зі своєю CRM, ERP або іншою інформаційною системою;
- передає запити через API;

- використовує Perevir як технічний інструмент внутрішнього комплаєнсу.

5.7.У ролі розпорядника або обробника Perevir:

- діє лише на підставі документованих вказівок корпоративного Користувача;
- обробляє лише необхідні категорії даних;
- забезпечує конфіденційність уповноважених осіб;
- застосовує належні заходи безпеки;
- залучає субпроцесорів відповідно до умов договору;
- сприяє виконанню запитів суб’єктів даних;
- повідомляє про виявлені інциденти;
- видаляє або повертає дані після припинення послуг, якщо інше не вимагається законом.

5.8.Конкретні умови обробки Perevir як обробником можуть встановлюватися окремим договором про обробку персональних даних - Data Processing Agreement.

Такий договір може визначати:

- предмет і строк обробки;
- характер та цілі операцій;
- категорії персональних даних;
- категорії суб’єктів даних;
- права й обов’язки сторін;
- умови залучення субпроцесорів;
- порядок міжнародного передавання;
- правила видалення та повернення даних;
- заходи інформаційної безпеки;
- порядок проведення перевірок та аудитів.

5.9. Perevir як самостійний контролер щодо похідної обробки

Perevir може виступати самостійним володільцем або контролером щодо окремих операцій із реєстровими та іншими законно отриманими даними, якщо Адміністрація самостійно визначає мету та способи:

- структурування інформації;
- уніфікації форматів;
- об’єднання даних із декількох джерел;
- створення графів зв’язків;
- формування часових ліній;
- створення аналітичних звітів;
- визначення технічних збігів;
- формування індикаторів ризику;
- виявлення аномалій;

- організації моніторингу змін.

5.10.Похідні аналітичні матеріали Perevir не змінюють зміст первинної інформації у відповідному державному чи іншому зовнішньому джерелі.

5.11.Аналітичний показник, індикатор ризику або автоматично сформований висновок Perevir:

- має інформаційний характер;
- не є офіційним рішенням державного органу;
- не встановлює юридичного факту;
- не замінює професійну юридичну, фінансову чи комплаєнс-оцінку;
- не повинен бути єдиною підставою для рішення, яке має істотні наслідки для фізичної особи.

5.12. Perevir як технічний посередник

Під час отримання інформації через державні шлюзи, зовнішні API, системи електронної ідентифікації або комерційні інформаційні сервіси Perevir може діяти як технічний посередник.

У такій ролі Perevir забезпечує:

- формування запиту;
- передавання запиту;
- отримання відповіді;
- перевірку технічного формату;
- відображення інформації;
- журналювання операції;
- захист каналу зв’язку.

5.13.Виконання технічної посередницької функції не означає, що Perevir:

- є держателем відповідного реєстру;
- визначає первинну мету ведення реєстру;
- відповідає за первинне внесення даних;
- має право самостійно виправляти офіційні відомості;
- набуває права власності на інформацію зовнішнього джерела.

5.14. Perevir як одержувач персональних даних

Perevir може бути одержувачем персональних даних, коли інформація передається:

- самим Користувачем;
- корпоративним Користувачем;
- засобом електронної ідентифікації;

- державним реєстром;
- постачальником API;
- платіжним провайдером;
- службою підтримки;
- іншою особою на законній підставі.

5.15.Отримання персональних даних не означає автоматичного права Perevir використовувати їх для будь-яких цілей.

Обробка обмежується метою, правовою підставою, умовами договору та вимогами законодавства.

5.16. Perevir і первинні володільці реєстрових даних

Стосовно державних реєстрів, офіційних інформаційних систем та відкритих наборів даних первинним володільцем, держателем або адміністратором є відповідний державний орган чи інша визначена законом особа.

Perevir може бути вторинним користувачем, одержувачем або окремим контролером похідної обробки, але не підміняє відповідного держателя реєстру.

5.17. Perevir і корпоративний Користувач як окремі контролери

У певних випадках Perevir та корпоративний Користувач можуть бути окремими самостійними володільцями або контролерами.

Це можливо, коли кожна сторона:

- самостійно визначає власну мету обробки;
- використовує дані для власної діяльності;
- самостійно визначає строки зберігання;
- окремо відповідає за права суб’єктів;
- не обробляє дані виключно за інструкцією іншої сторони.

5.18. Спільні контролери

Perevir і третя особа можуть виступати спільними контролерами лише тоді, коли вони фактично спільно визначають мету та істотні засоби конкретної обробки.

У такому разі сторони визначають розподіл обов’язків окремою угодою або іншим документом.

5.19. Залучення субпроцесорів

Коли Perevir виступає обробником, Адміністрація може залучати субпроцесорів для виконання окремих технічних операцій, зокрема:

- хостингу;
- хмарного зберігання;
- резервного копіювання;
- моніторингу;
- аналітики;
- комунікацій;
- електронної ідентифікації;
- кібербезпеки;
- технічної підтримки.

5.20.Субпроцесори повинні бути пов'язані вимогами щодо захисту даних, які за своїм змістом не є слабшими за вимоги, покладені на Perevir.

5.21. Зміна ролі залежно від операції

Perevir може одночасно виконувати різні ролі щодо різних наборів даних.

Наприклад:

- щодо даних облікового запису - бути контролером;
- щодо корпоративного списку моніторингу - бути обробником;
- щодо технічних журналів безпеки - бути контролером;
- щодо даних державного реєстру - бути одержувачем і самостійним контролером похідної обробки;
- щодо окремого зовнішнього API - бути технічним посередником.

5.22.Роль Perevir у конкретному випадку може додатково визначатися:

- повідомленням під час збирання даних;
- умовами функціонального модуля;
- договором;
- Data Processing Agreement;
- правилами API;
- документацією інтеграції;
- цією Політикою;
- застосовним законодавством.

5.23.Якщо характер конкретної операції не дозволяє однозначно визначити роль Perevir, Адміністрація проводить оцінку з урахуванням фактичного розподілу повноважень, мети обробки та контролю над істотними засобами обробки.

6. Джерела інформації

6.1. Для надання інформаційно-аналітичних функцій Perevir може отримувати, використовувати, систематизувати, зіставляти та відображати інформацію з державних, офіційних, публічних, відкритих, договірних та інших законних джерел.

6.2. Perevir не є первинним автором, реєстратором або володільцем більшості відомостей, що отримуються із зовнішніх інформаційних ресурсів. Система забезпечує технічний пошук, одержання, структурування, зіставлення, візуалізацію, аналітичне опрацювання та відображення інформації в межах, дозволених законодавством і правилами відповідного джерела.

6.3. Залежно від доступної функціональності, правового режиму інформації та технічної можливості доступу Perevir може використовувати інформацію, зокрема, з таких джерел:

- **Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань - ЄДР**, зокрема відомості про:
    - юридичних осіб;
    - фізичних осіб - підприємців;
    - громадські формування;
    - керівників;
    - засновників та учасників;
    - кінцевих бенефіціарних власників;
    - види економічної діяльності;
    - стан юридичної особи або ФОП;
    - реєстраційні зміни;
    - інші відомості, доступні відповідно до законодавства.
- **Автоматизованої системи виконавчого провадження - АСВП**, включаючи доступні відомості про виконавчі провадження, боржників та іншу інформацію, відкритість якої передбачена законодавством.
- **Інформаційних ресурсів Державної податкової служби України - ДПС**, зокрема відомості про:
    - податковий статус;
    - реєстрацію платником податків;
    - реєстрацію платником податку на додану вартість;
    - податковий борг;
    - анульовані або чинні реєстрації;
    - інші загальнодоступні податкові відомості.
- **Інформаційних ресурсів Національної комісії з цінних паперів та фондового ринку - НКЦПФР**, зокрема відомості про емітентів, професійних учасників ринків капіталу, фінансову звітність, власників істотної участі та іншу інформацію, оприлюднену відповідно до законодавства.
- **Єдиного державного реєстру судових рішень та інших ресурсів судової влади України**, зокрема відомості про:
    - судові рішення;

    - стан розгляду судових справ;
    - учасників судових проваджень;
    - призначені судові засідання;
    - інші дані, доступні на офіційних ресурсах судової влади.
- **Електронної системи публічних закупівель Prozorro**, включаючи відомості про:
    - учасників і замовників закупівель;
    - тендерні пропозиції;
    - договори;
    - результати закупівель;
    - скарги;
    - кваліфікаційні рішення;
    - інші документи та події закупівель.
- **Єдиного державного вебпорталу відкритих даних та інших державних порталів відкритих даних**, включаючи набори даних, оприлюднені розпорядниками публічної інформації у формі відкритих даних.
- **Державного реєстру речових прав на нерухоме майно та пов'язаних із ним інформаційних ресурсів**, якщо доступ до відповідних відомостей є законним, технічно доступним і передбачений функціональністю Perevir.
- **Державних реєстрів, переліків і баз даних у сфері санкцій, банкрутства, ліцензування, дозвільної діяльності, фінансового моніторингу та регуляторного контролю**, якщо відповідні відомості є відкритими або доступ до них отриманий на належній правовій підставі.
- **Офіційних вебсайтів державних органів, органів місцевого самоврядування, судів, регуляторів та інших суб'єктів владних повноважень**.
- **Комерційних інформаційних систем та постачальників даних**, зокрема через YouControl API, якщо відповідна інтеграція буде впроваджена та використання даних здійснюватиметься на підставі договору, ліцензії або іншої належної правової підстави.
- **Інших джерел**, використання яких не заборонене законодавством і відповідає меті функціонування Perevir.

6.4. Наведений перелік не є вичерпним. Конкретний перелік джерел може залежати від:

- обраного тарифного плану;
- доступної функціональності;
- типу звіту;
- правового статусу Користувача;
- проходження електронної ідентифікації;
- встановлених законодавством обмежень;
- технічної доступності відповідного джерела;
- умов договорів із постачальниками інформації.

6.5. Perevir використовує лише ті способи доступу до інформації, які є законними та технічно дозволеними, зокрема:

- офіційні API;
- державні електронні сервіси;
- договори інформаційної взаємодії;
- ліцензовані комерційні API;
- відкриті набори даних;
- офіційні публічні вебресурси;
- інші правомірні канали отримання інформації.

6.6. Якщо відповідне джерело встановлює спеціальні умови, обмеження, тарифи, квоти, правила ідентифікації або вимоги щодо мети доступу, Perevir обробляє та надає відповідну інформацію з урахуванням таких умов.

6.7. Доступ до окремих категорій інформації може бути обмежений залежно від:

- вимог законодавства;
- правового режиму відповідного реєстру;
- проходження Користувачем електронної ідентифікації;
- підтвердження законної мети доступу;
- рішень держателя або адміністратора реєстру;
- дії воєнного чи надзвичайного стану;
- санкційних та інших регуляторних обмежень.

6.8. Perevir не змінює зміст первинних офіційних відомостей на власний розсуд.

Водночас Система може:

- структурувати інформацію;
- об’єднувати відомості з декількох джерел;
- приводити дані до єдиного формату;
- створювати графи зв’язків;
- формувати часові лінії;
- визначати технічні збіги;
- формувати індикатори ризику;
- створювати аналітичні звіти та узагальнення.

Такі результати є похідними інформаційно-аналітичними матеріалами Perevir і не змінюють зміст первинних даних у відповідному офіційному джерелі.

6.9.Інформація з різних джерел може відрізнятися через:

- різний час оновлення;
- технічні затримки;

- помилки первинного джерела;
- відмінності у форматах;
- обмеження доступу;
- неповноту оприлюднених відомостей;
- зміни законодавства;
- тимчасову недоступність відповідного ресурсу.

У разі розбіжностей юридично значущу інформацію необхідно перевіряти безпосередньо у відповідному офіційному джерелі.

6.10. Perevir може фіксувати технічні метадані про джерело отримання інформації, зокрема:

- назву джерела;
- дату й час отримання;
- дату оновлення набору даних, якщо вона доступна;
- ідентифікатор запиту;
- версію або формат отриманих даних;
- інші відомості, необхідні для аудиту, безпеки та підтвердження походження інформації.

6.11.Отримання інформації з публічного або відкритого джерела не означає, що така інформація може надалі використовуватися без будь-яких обмежень.

Користувач зобов’язаний враховувати:

- мету первинного оприлюднення;
- вимоги законодавства про захист персональних даних;
- права та законні інтереси фізичних осіб;
- обмеження щодо поширення інформації;
- права інтелектуальної власності;
- правила відповідного інформаційного ресурсу.

6.12.Користувачу забороняється використовувати інформацію, отриману через Perevir, для:

- незаконного переслідування;
- дискримінації;
- шантажу;
- шахрайства;
- спаму;
- незаконного профілювання;
- порушення приватності;
- протиправного поширення персональних даних;
- обходу обмежень державних реєстрів;

- іншої незаконної діяльності.

6.13.Підключення нового джерела, тимчасове припинення його використання або зміна способу доступу до нього не обов’язково потребує внесення змін до цієї Політики, якщо при цьому істотно не змінюються категорії персональних даних, цілі або правові підстави їх обробки.

6.14.Якщо підключення нового джерела призводить до істотної зміни характеру обробки персональних даних, Адміністрація оновлює цю Політику та, якщо цього вимагає законодавство, надає Користувачам відповідне повідомлення або отримує необхідну згоду.

7. Категорії інформації та персональних даних

7.1.Обсяг і категорії інформації, яку обробляє Perevir, залежать від:

- способу використання Системи;
- статусу Користувача;
- обраного тарифного плану;
- доступної функціональності;
- використання електронної ідентифікації;
- підключених інтеграцій;
- джерел інформації;
- налаштувань моніторингу;
- змісту договору з корпоративним Користувачем.

7.2. Perevir дотримується принципу мінімізації та прагне обробляти лише ті персональні дані, які є належними, релевантними й необхідними для досягнення визначених цілей.

7.3. Реєстраційні дані. Під час створення та використання облікового запису Perevir можуть оброблятися:

- адреса електронної пошти;
- пароль у захищеному або криптографічно перетвореному вигляді;
- ім’я та прізвище, якщо вони надаються Користувачем;
- номер телефону, якщо його надання передбачене функціональністю;
- назва організації;
- посада;
- підрозділ;
- службові контактні дані;
- мова інтерфейсу;
- країна або регіон;
- інші дані профілю, добровільно надані Користувачем.

7.4. Perevir не має доступу до пароля Користувача у відкритому вигляді та не зберігає його у формі, що дозволяє безпосередньо прочитати пароль.

7.5. Дані електронної ідентифікації

Під час проходження електронної ідентифікації за допомогою КЕП, Дія.Підпис або іншого передбаченого законодавством засобу Perevir може отримувати:

- прізвище, власне ім’я та по батькові;
- РНОКПП;
- серію та номер документа, якщо такі відомості надаються відповідним засобом і є необхідними;
- дату народження, якщо вона необхідна для ідентифікації;
- найменування юридичної особи;
- код ЄДРПОУ;
- посаду або статус представника;
- відомості про сертифікат відкритого ключа;
- найменування кваліфікованого надавача електронних довірчих послуг;
- строк чинності сертифіката;
- результат і дату проходження ідентифікації;
- унікальний технічний ідентифікатор операції;
- інші мінімально необхідні ідентифікаційні атрибути.

7.6. Perevir не зберігає:

- особисті ключі КЕП;
- паролі захисту особистих ключів;
- файли ключів, якщо їх зберігання не є технічно необхідним для окремо погодженої функції;
- біометричні шаблони, які використовуються застосунком «Дія» або іншим постачальником для підтвердження особи.

Ідентифікація і створення електронного підпису здійснюються через відповідного надавача електронних довірчих послуг, державну інформаційну систему або застосунок «Дія». Наявна редакція політики Perevir також передбачає, що Система не зберігає приватні ключі КЕП та паролі до них.

7.7. Дані корпоративного Користувача

Якщо доступ до Perevir надається юридичній особі, фізичній особі - підприємцю або іншій організації, можуть оброблятися:

- повне та скорочене найменування;
- код ЄДРПОУ або інший реєстраційний номер;
- податкові реквізити;

- юридична та поштова адреса;
- платіжні реквізити;
- контактні дані уповноважених осіб;
- посади та повноваження представників;
- список користувачів корпоративного облікового запису;
- ролі й рівні доступу;
- інформація про договір;
- тарифний план;
- рахунки, акти та інші розрахункові документи.

Відомості про юридичну особу самі по собі можуть не бути персональними даними. Водночас дані її працівників, представників, засновників, керівників і бенефіціарних власників можуть належати до персональних даних.

7.8. Дані про використання облікового запису

Perevir може обробляти:

- дату й час створення облікового запису;
- дату й час входу та виходу;
- історію успішних і невдалих спроб входу;
- статус облікового запису;
- налаштування профілю;
- обраний тариф;
- інформацію про активацію функцій;
- ролі та дозволи;
- історію зміни пароля;
- факти проходження електронної ідентифікації;
- згоду або відмову від окремих налаштувань;
- історію прийняття Правил і Політики;
- інші події, необхідні для адміністрування та захисту облікового запису.

7.9. Дані про пошукові запити та перевірки

Під час використання інформаційно-аналітичних функцій можуть оброблятися:

- введені пошукові критерії;
- назва юридичної особи;
- код ЄДРПОУ;
- ПІБ фізичної особи;
- РНОКПП, якщо його використання дозволено законом;
- номер судової справи;
- номер виконавчого провадження;
- реєстраційні та інші ідентифікатори;
- дата й час запиту;

- джерело отриманої інформації;
- тип сформованого звіту;
- результати пошуку;
- історія переглянутих звітів;
- обрані фільтри;
- експортовані або завантажені документи;
- інші параметри запиту.

7.10.Історія запитів може містити персональні дані осіб, яких перевіряє Користувач. Тому доступ до такої історії надається лише уповноваженим Користувачам відповідного облікового запису та іншим особам, які мають належну правову підставу.

7.11. Дані моніторингу

Якщо Користувач використовує функцію моніторингу, Perevir може обробляти:

- перелік юридичних осіб, ФОП або інших суб’єктів моніторингу;
- ідентифікатори таких суб’єктів;
- налаштування відстежуваних подій;
- дату додавання до моніторингу;
- дату та зміст виявленої зміни;
- канали й адреси надсилання повідомлень;
- статус доставки повідомлення;
- історію повідомлень;
- налаштування періодичності перевірок.

7.12. Реєстрові та інші зовнішні дані

Perevir може обробляти інформацію, отриману з державних, офіційних, відкритих, договірних та інших законних джерел, зокрема:

- реєстраційні відомості про юридичних осіб і ФОП;
- відомості про керівників, засновників, учасників та бенефіціарних власників;
- дані про виконавчі провадження;
- податкову інформацію, доступну на законній підставі;
- відомості про судові справи та судові рішення;
- дані про публічні закупівлі;
- ліцензії та дозволи;
- санкційні відомості;
- інформацію про банкрутство;
- регуляторну інформацію;
- відомості про цінні папери та ринки капіталу;
- інші дані, доступні відповідно до законодавства та умов джерела.

7.13.Реєстрові та зовнішні дані можуть містити персональні дані третіх осіб, зокрема:

- ПІБ;
- дату народження;
- відомості про підприємницьку або професійну діяльність;
- місце роботи та посаду;
- відомості про участь у юридичних особах;
- судову та виконавчу інформацію;
- відомості про право власності;
- контактні або адресні дані, якщо їх оприлюднення чи надання дозволено законом;
- інші відомості, що стосуються ідентифікованої або такої, яку можна ідентифікувати, фізичної особи.

7.14. Perevir не вважає будь-яку інформацію з відкритого джерела такою, що може використовуватися без обмежень. До неї застосовуються вимоги щодо законності, мети, пропорційності, захисту персональних даних і прав відповідних осіб.

7.15. Інформаційно-аналітичні та похідні дані

На основі законно отриманої інформації Perevir може створювати:

- структуровані профілі;
- інформаційні звіти;
- зведені таблиці;
- часові лінії;
- графи зв’язків;
- порівняльні матеріали;
- індикатори ризику;
- повідомлення про зміни;
- технічні збіги;
- результати зіставлення;
- інші похідні аналітичні матеріали.

7.16.Похідні аналітичні матеріали можуть містити персональні дані або давати можливість зробити висновки про фізичну особу. До таких матеріалів застосовуються вимоги щодо захисту персональних даних у тому самому обсязі, що й до первинних даних, якщо інше не передбачено законом.

7.17. Технічні дані

Під час відвідування вебсайту або використання Perevir можуть автоматично оброблятися:

- IP-адреса;
- дата й час з’єднання;
- тип і версія браузера;

- тип пристрою;
- операційна система;
- мова та регіональні налаштування;
- ідентифікатори пристрою або сесії;
- адреса сторінки, з якої здійснений перехід;
- переглянуті сторінки;
- тривалість сесії;
- дії в інтерфейсі;
- технічні помилки;
- журнали системних подій;
- дані про продуктивність;
- відомості про мережеві запити;
- ознаки автоматизованого або аномального використання.

7.18. Cookies та подібні технології

Perevir може використовувати:

- обов’язкові cookies;
- cookies автентифікації;
- cookies безпеки;
- cookies збереження налаштувань;
- аналітичні cookies;
- локальне сховище браузера;
- ідентифікатори сесії;
- інші подібні технології.

Детальні умови їх застосування можуть визначатися окремою Політикою використання cookies.

7.19. Дані комунікацій

Коли Користувач звертається до Адміністрації, можуть оброблятися:

- ПІБ;
- електронна адреса;
- номер телефону;
- назва організації;
- тема звернення;
- текст повідомлення;
- вкладені файли;
- дата й час звернення;
- історія листування;
- записи звернень до підтримки;
- оцінка якості обслуговування;

- інші відомості, добровільно надані Користувачем.

7.20. Платіжна та розрахункова інформація

Під час придбання платних послуг можуть оброблятися:

- інформація про платника;
- назва та реквізити юридичної особи або ФОП;
- адреса для виставлення рахунків;
- податкові реквізити;
- номер і дата рахунку;
- сума та валюта платежу;
- статус платежу;
- тарифний план;
- строк підписки;
- номер платіжної операції;
- дані актів, рахунків та інших бухгалтерських документів.

7.21.Повні реквізити платіжної картки можуть оброблятися безпосередньо банком, платіжною системою або платіжним провайдером. Perevir може отримувати лише обмежену технічну інформацію про операцію, якщо інше прямо не зазначено під час оплати.

7.22. Дані інформаційної безпеки

З метою захисту Системи можуть оброблятися:

- журнали автентифікації;
- невдалі спроби входу;
- IP-адреси;
- відомості про підозрілі дії;
- сигнали систем захисту;
- дані про блокування;
- ознаки використання ботів або скриптів;
- інформація про порушення лімітів;
- результати внутрішніх розслідувань;
- дані про інциденти;
- відомості, необхідні для захисту прав Адміністрації та Користувачів.

7.23. Відгуки та матеріали Користувачів

Perevir може обробляти:

- відгуки;
- пропозиції;

- результати опитувань;
- повідомлення про помилки;
- коментарі щодо бета-функцій;
- приклади проблемних запитів;
- інші матеріали, надані для вдосконалення Системи.

7.24. Спеціальні категорії персональних даних

Perevir не призначений для цілеспрямованого збирання спеціальних категорій персональних даних, зокрема даних про:

- расове або етнічне походження;
- політичні переконання;
- релігійні чи світоглядні переконання;
- членство у професійних спілках;
- генетичні дані;
- біометричні дані для унікальної ідентифікації;
- стан здоров’я;
- статеве життя або сексуальну орієнтацію.

7.25.Окремі відомості такої категорії можуть випадково міститися в судових рішеннях, офіційних документах або матеріалах, отриманих із законного зовнішнього джерела.

У такому разі Perevir застосовує додаткові обмеження та обробляє їх лише за наявності належної правової підстави.

7.26. Дані про правопорушення та судимості

Інформація про кримінальні правопорушення, судимості, кримінальні провадження або інші правопорушення може оброблятися лише:

- у межах офіційно оприлюдненої інформації;
- якщо доступ до неї дозволений законом;
- для законної та визначеної мети;
- із дотриманням встановлених обмежень;
- без створення необґрунтованих або дискримінаційних висновків.

7.27.Користувачу заборонено завантажувати або передавати до Perevir надмірні, незаконно отримані чи не пов’язані з метою використання персональні дані.

8. Як ми отримуємо персональні дані

8.1. Perevir може отримувати персональні дані:

- безпосередньо від Користувача;
- від корпоративного Користувача;
- автоматично під час використання Системи;
- через засоби електронної ідентифікації;
- з державних реєстрів та офіційних ресурсів;
- із відкритих даних;
- від комерційних постачальників інформації;
- через API та інтеграції;
- від постачальників технічних і платіжних послуг;
- з інших законних джерел.

Загальна політика Binotel також передбачає отримання персональних даних безпосередньо від особи під час використання сервісів або через використання сервісів клієнтами.

8.2. Безпосередньо від Користувача

Ми отримуємо дані безпосередньо від Користувача, коли він:

- створює обліковий запис;
- заповнює профіль;
- укладає договір;
- оформлює підписку;
- здійснює оплату;
- проходить ідентифікацію;
- вводить пошуковий запит;
- додає суб’єкта до моніторингу;
- налаштовує повідомлення;
- звертається до підтримки;
- бере участь в опитуванні;
- повідомляє про помилку;
- тестує бета-функцію;
- іншим способом взаємодіє з Perevir.

8.3.Надання окремих персональних даних може бути:

- обов’язковим для створення облікового запису;
- необхідним для укладення або виконання договору;
- потрібним для доступу до певної інформації;
- передбаченим законодавством;
- добровільним.

8.4.Якщо Користувач не надає обов’язкові дані, Perevir може не мати можливості:

- створити обліковий запис;

- підтвердити особу;
- надати доступ до відповідної функції;
- сформувати звіт;
- виконати платіж;
- відповісти на звернення;
- виконати інше запитане обслуговування.

8.5. Від корпоративного Користувача

Корпоративний Користувач може передавати Perevir дані своїх:

- працівників;
- адміністраторів облікового запису;
- уповноважених представників;
- контрагентів;
- клієнтів;
- кандидатів;
- інших фізичних осіб, перевірка або моніторинг яких здійснюється на законній підставі.

8.6.Корпоративний Користувач зобов’язаний забезпечити законність такого передавання та виконати обов’язки володільця або контролера даних, зокрема щодо правової підстави, інформування суб’єктів і мінімізації даних.

8.7. Через електронну ідентифікацію

Під час використання КЕП, Дія.Підпис або іншого засобу електронної ідентифікації Perevir може отримувати від відповідного надавача:

- підтвердження успішної або неуспішної ідентифікації;
- ідентифікаційні атрибути;
- відомості із сертифіката;
- технічний ідентифікатор операції;
- дату й час операції;
- інші відомості, необхідні для підтвердження особи.

8.8.Склад отриманих даних залежить від:

- типу засобу ідентифікації;
- налаштувань відповідного державного або приватного сервісу;
- законодавчих вимог;
- мети ідентифікації;
- обсягу інформації, дозволеного Користувачем.

8.9. Perevir не отримує та не зберігає особистий ключ КЕП або пароль до нього. Наявна політика Perevir прямо передбачає, що ідентифікація здійснюється через захищені державні шлюзи, відповідного провайдера або застосунок «Дія».

8.10. Автоматично під час використання Perevir

Певні технічні дані збираються автоматично, коли Користувач:

- відкриває вебсайт;
- входить до облікового запису;
- переглядає сторінки;
- формує запит;
- використовує функцію;
- завантажує звіт;
- взаємодіє з повідомленням;
- здійснює інші дії в Системі.

8.11.Автоматичний збір може здійснюватися за допомогою:

- серверних журналів;
- cookies;
- локального сховища браузера;
- ідентифікаторів сесії;
- систем моніторингу доступності;
- систем виявлення помилок;
- засобів інформаційної безпеки;
- аналітичних технологій;
- інших технічних засобів.

8.12. Із державних реєстрів та офіційних ресурсів

Perevir може отримувати інформацію через:

- офіційні API;
- державні електронні сервіси;
- відкриті набори даних;
- вебпортали державних органів;
- системи електронної взаємодії;
- договори інформаційного обміну;
- інші законні технічні канали.

8.13.До відповідних джерел можуть належати:

- ЄДР;
- АСВП;

- ресурси ДПС;
- ресурси НКЦПФР;
- Єдиний державний реєстр судових рішень;
- інші ресурси судової влади;
- Prozorro;
- Єдиний державний вебпортал відкритих даних;
- інші державні та офіційні ресурси.

Конкретний перелік джерел визначається розділом «Джерела інформації» цієї Політики.

8.14. Із комерційних та договірних джерел

Perevir може отримувати інформацію від комерційних постачальників, зокрема через:

- ліцензовані бази даних;
- інформаційні платформи;
- API;
- партнерські інтеграції;
- договірні канали обміну.

8.15.До таких постачальників може належати YouControl, якщо відповідна інтеграція буде впроваджена та використовуватиметься на підставі чинного договору, ліцензії або іншої належної правової підстави.

8.16. Від платіжних і фінансових постачальників

Під час оплати ми можемо отримувати від банку, платіжного сервісу або іншого постачальника:

- підтвердження платежу;
- суму;
- валюту;
- дату й час;
- статус операції;
- ідентифікатор транзакції;
- обмежені відомості про спосіб оплати;
- інформацію, необхідну для бухгалтерського та податкового обліку.

8.17. Від постачальників технічних послуг

Perevir може отримувати технічні відомості від постачальників:

- хостингу;
- хмарної інфраструктури;
- електронної пошти;

- аналітики;
- моніторингу;
- кібербезпеки;
- служби підтримки;
- електронної ідентифікації;
- інших технічних сервісів.

8.18. Від інших Користувачів та третіх осіб

Інша особа може надати відомості про Користувача, наприклад коли:

- корпоративний адміністратор створює для нього доступ;
- представник організації передає контактні дані;
- особу додають до робочої групи;
- дані містяться у зверненні або вкладеному документі;
- інша особа повідомляє про можливе порушення безпеки чи Правил.

8.19.Якщо персональні дані отримані не безпосередньо від суб'єкта, Perevir надає передбачену законодавством інформацію про обробку, крім випадків, коли:

- суб'єкт уже має відповідну інформацію;
- надання інформації є неможливим або потребує непропорційних зусиль;
- отримання чи розкриття прямо передбачене законом;
- застосовується інший передбачений законодавством виняток.

8.20. Perevir не використовує незаконні способи одержання персональних даних і не здійснює доступ до інформації шляхом обходу технічних, правових або організаційних обмежень відповідного джерела.

9. Цілі обробки персональних даних

9.1. Perevir обробляє персональні дані лише для визначених, конкретних і законних цілей.

Подальша обробка не повинна бути несумісною з метою, для якої дані були отримані, крім випадків, дозволених законодавством.

9.2. Реєстрація та адміністрування облікового запису

Персональні дані обробляються для:

- створення облікового запису;
- підтвердження електронної адреси;
- автентифікації Користувача;

- відновлення доступу;
- керування профілем;
- призначення ролей і прав доступу;
- адміністрування корпоративного кабінету;
- ведення історії істотних змін облікового запису.

9.3. Укладення та виконання договору

Дані обробляються для:

- вчинення дій до укладення договору;
- оформлення замовлення;
- активації тарифу;
- надання доступу до функціональності;
- виконання договірних зобов’язань;
- адміністрування підписки;
- підготовки рахунків, актів та інших документів;
- супроводу договірних відносин;
- припинення або поновлення послуг.

9.4. Електронна ідентифікація

Персональні дані можуть оброблятися для:

- підтвердження особи Користувача;
- підтвердження повноважень представника;
- виконання вимог законодавства;
- надання доступу до інформації з обмеженим режимом перегляду;
- запобігання несанкціонованому доступу;
- фіксації факту та результату ідентифікації;
- забезпечення доказовості відповідної електронної операції.

9.5. Надання інформаційно-аналітичних функцій

Дані обробляються для:

- виконання пошукових запитів;
- отримання інформації із законних джерел;
- структурування й систематизації відомостей;
- зіставлення інформації з різних джерел;
- формування звітів;
- створення графів зв’язків;
- побудови часових ліній;
- визначення технічних збігів;
- формування індикаторів ризику;

- відображення історії змін;
- надання іншої функціональності Perevir.

9.6. Перевірка контрагентів і комплаєнс

Perevir може забезпечувати технічні інструменти для:

- перевірки юридичних осіб та ФОП;
- перевірки реєстраційного статусу;
- аналізу корпоративних зв'язків;
- санкційної перевірки;
- перевірки судової та виконавчої інформації;
- аналізу участі у публічних закупівлях;
- виявлення регуляторних і репутаційних факторів;
- оцінювання ризиків співпраці.

9.7. Perevir не визначає самостійно законну мету конкретної перевірки, яку проводить Користувач у межах своєї діяльності.

Користувач відповідає за законність перевірки, належну правову підставу та використання її результатів.

9.8. Моніторинг і повідомлення

Дані обробляються для:

- створення списків моніторингу;
- періодичної перевірки змін;
- виявлення нових реєстрових подій;
- порівняння попередніх і актуальних відомостей;
- формування повідомлень;
- надсилання повідомлень електронною поштою або іншим обраним каналом;
- ведення історії змін та сповіщень.

9.9. Персоналізація роботи Системи

Дані можуть використовуватися для:

- збереження мови та інших налаштувань;
- відображення доступної функціональності;
- налаштування робочого простору;
- формування історії запитів;
- збереження фільтрів;
- налаштування повідомлень;
- адаптації інтерфейсу до ролі Користувача.

9.10. Надання технічної підтримки

Персональні дані обробляються для:

- прийняття й опрацювання звернень;
- ідентифікації Користувача;
- діагностики проблем;
- відтворення помилки;
- відновлення доступу;
- надання консультацій;
- контролю якості підтримки;
- документування вирішення звернення.

9.11. Комунікація з Користувачем

Ми можемо використовувати контактні дані для надсилання:

- сервісних повідомлень;
- повідомлень про стан облікового запису;
- повідомлень про безпеку;
- повідомлень про зміни в моніторингу;
- інформації про технічні роботи;
- відповідей на звернення;
- повідомлень про зміну Правил або Політики;
- рахунків та інших договірних документів.

9.12.Сервісні й безпекові повідомлення не вважаються маркетинговими та можуть надсилатися, якщо вони необхідні для надання послуг, захисту облікового запису або виконання законодавчих обов’язків.

9.13. Маркетингові комунікації

За наявності належної правової підстави контактні дані можуть використовуватися для:

- надсилання інформації про нові функції;
- повідомлень про спеціальні пропозиції;
- запрошень до тестування;
- проведення опитувань;
- надсилання інших маркетингових матеріалів.

9.14.Користувач може відмовитися від маркетингових повідомлень за допомогою:

- посилання для відписки;
- налаштувань облікового запису;
- звернення до Адміністрації.

Відмова від маркетингових повідомлень не припиняє надсилання необхідних сервісних і безпекових повідомлень.

9.15. Оплата, бухгалтерський і податковий облік

Дані обробляються для:

- виставлення рахунків;
- приймання й підтвердження платежів;
- ведення обліку;
- формування актів;
- повернення коштів;
- виконання податкових і бухгалтерських вимог;
- розгляду платіжних спорів;
- запобігання платіжному шахрайству.

9.16. Інформаційна безпека

Персональні й технічні дані обробляються для:

- захисту облікових записів;
- контролю доступу;
- виявлення несанкціонованих дій;
- виявлення автоматизованого збирання інформації;
- запобігання шахрайству;
- протидії атакам;
- розслідування інцидентів;
- журналювання;
- резервного копіювання;
- відновлення після збоїв;
- забезпечення безперервності роботи;
- захисту прав і законних інтересів Адміністрації та Користувачів.

9.17. Запобігання незаконному використанню

Дані можуть оброблятися для:

- перевірки дотримання Правил;
- виявлення спільного використання облікових записів;
- виявлення ботів, скриптів, парсерів і краулерів;
- контролю технічних лімітів;
- виявлення спроб обходу обмежень;
- блокування підозрілої активності;
- документування порушень;
- захисту від претензій і зловживань.

9.18. Виконання вимог законодавства

Дані можуть оброблятися для:

- виконання законодавчих і регуляторних обов’язків;
- відповіді на законні вимоги компетентних органів;
- виконання судових рішень;
- санкційної та комплаєнс-перевірки;
- дотримання вимог експортного контролю;
- зберігання обов’язкової документації;
- виконання інших вимог застосовного права.

9.19. Встановлення, реалізація та захист правових вимог

Дані можуть зберігатися й використовуватися для:

- досудового врегулювання спорів;
- підготовки претензій;
- захисту в суді;
- доказування фактів використання Системи;
- стягнення заборгованості;
- розслідування порушень;
- захисту інтелектуальної власності;
- виконання договірних прав і обов’язків.

9.20. Удосконалення Perevir

Дані можуть оброблятися для:

- аналізу використання функцій;
- виявлення помилок;
- оцінювання продуктивності;
- тестування оновлень;
- оптимізації інтерфейсу;
- розроблення нових функцій;
- аналізу зворотного зв’язку;
- підвищення точності пошуку;
- удосконалення інформаційно-аналітичних алгоритмів.

9.21.Для розвитку та тестування переважно використовуються:

- знеособлені дані;
- агрегована статистика;
- синтетичні дані;
- тестові набори;
- мінімально необхідний обсяг реальних даних.

Використання персональних даних для розроблення та тестування допускається лише за наявності належної правової підстави та відповідних заходів захисту.

9.22. Аналітика роботи Системи

Технічні дані можуть оброблятися для:

- статистики відвідувань;
- аналізу навантаження;
- оцінювання популярності функцій;
- виявлення проблемних сценаріїв;
- аналізу конверсій;
- планування ресурсів;
- формування внутрішньої звітності.

9.23. Тестування бета-функцій

Під час використання бета-функцій дані можуть оброблятися для:

- перевірки стабільності;
- виявлення помилок;
- оцінювання якості;
- аналізу сценаріїв використання;
- перевірки сумісності;
- отримання зворотного зв’язку;
- прийняття рішення про подальший розвиток функції.

9.24. Корпоративні зміни

Персональні дані можуть оброблятися у зв’язку з:

- реорганізацією;
- злиттям;
- поділом;
- перетворенням;
- продажем підприємства або його частини;
- передаванням прав на Систему;
- залученням інвестора;
- проведенням юридичного, фінансового або безпекового аудиту.

У такому разі застосовуються вимоги конфіденційності, мінімізації та законності передавання.

9.25.Якщо Адміністрація планує використовувати персональні дані для нової мети, яка не є сумісною з первинною, вона:

- визначає належну правову підставу;
- оцінює вплив на права суб’єктів;
- оновлює цю Політику або надає окреме повідомлення;
- отримує згоду, якщо вона необхідна;
- застосовує додаткові заходи захисту.

9.26. Perevir не використовує персональні дані для прихованих або незаконних цілей і не продає персональні дані Користувачів третім особам для їхнього незалежного маркетингового використання.

10. Правові підстави обробки персональних даних

10.1. Perevir обробляє персональні дані лише за наявності належної правової підстави, визначеної законодавством України та, якщо застосовується, законодавством Європейського Союзу про захист персональних даних.

10.2.Конкретна правова підстава залежить від:

- категорії персональних даних;
- суб’єкта персональних даних;
- джерела отримання інформації;
- мети обробки;
- ролі Perevir у відповідній операції;
- умов договору з Користувачем;
- режиму доступу до відповідного реєстру або інформаційного джерела;
- застосовного законодавства.

10.3. Виконання договору

Perevir може обробляти персональні дані, якщо це необхідно для:

- укладення договору з Користувачем;
- вчинення дій на запит Користувача до укладення договору;
- створення облікового запису;
- надання доступу до Системи;
- активації тарифного плану;
- надання інформаційно-аналітичних функцій;
- здійснення розрахунків;
- технічної підтримки;
- виконання інших договірних зобов’язань.

10.4.Якщо без обробки певних персональних даних неможливо виконати договір або надати запитану функцію, відмова від надання таких даних може призвести до

неможливості створення облікового запису, ідентифікації Користувача або надання відповідної послуги.

10.5. Виконання вимог законодавства

Персональні дані можуть оброблятися, якщо така обробка необхідна для виконання обов'язку, покладеного на Адміністрацію законодавством, зокрема для:

- бухгалтерського та податкового обліку;
- зберігання обов'язкової документації;
- виконання судових рішень;
- відповіді на законні вимоги компетентних органів;
- дотримання санкційних та інших регуляторних вимог;
- забезпечення належного рівня інформаційної безпеки;
- виконання вимог щодо електронної ідентифікації;
- запобігання незаконному доступу до інформації.

Закон України «Про захист персональних даних» допускає обробку персональних даних на підставах, визначених законом, а законодавство про електронну ідентифікацію окремо передбачає необхідність захисту даних, що обробляються під час надання відповідних послуг.

10.6. Дозвіл, наданий законом

Perevir може обробляти персональні дані без окремої згоди суб'єкта, якщо обробка прямо дозволена законом і здійснюється виключно для виконання передбачених законом повноважень, обов'язків або законних функцій.

10.7.Наявність персональних даних у державному реєстрі, судовому рішенні, відкритому наборі даних або іншому офіційному джерелі не скасовує вимог щодо законності, визначеності мети, пропорційності та безпеки їх подальшої обробки.

10.8. Законний інтерес

Perevir може обробляти персональні дані для реалізації власного законного інтересу або законного інтересу третьої особи за умови, що права, свободи та законні інтереси суб'єкта персональних даних не мають переваги над таким інтересом.

10.9.До законних інтересів Perevir можуть належати:

- забезпечення безпеки Системи;
- запобігання шахрайству та зловживанням;
- захист облікових записів;
- журналювання та аудит;
- забезпечення стабільності й безперервності роботи;

- удосконалення функціональності;
- захист прав Адміністрації;
- встановлення, реалізація або захист правових вимог;
- ведення внутрішньої статистики;
- запобігання несанкціонованому автоматизованому збору інформації.

10.10.Перед обробкою на підставі законного інтересу Адміністрація може оцінювати:

- законність і конкретність такого інтересу;
- необхідність обробки;
- можливість досягнення мети менш втручальним способом;
- обсяг і характер даних;
- обґрунтовані очікування суб'єкта;
- ризик негативного впливу на його права;
- необхідні заходи захисту.

10.11. Згода суб'єкта персональних даних

Perevir може обробляти персональні дані на підставі добровільної, конкретної, поінформованої та однозначної згоди суб'єкта.

10.12.Згода може використовуватися, зокрема, для:

- надсилання маркетингових повідомлень;
- використання необов'язкових аналітичних cookies;
- участі в окремих дослідженнях або опитуваннях;
- тестування окремих функцій;
- обробки даних у випадках, коли інша належна правова підстава відсутня.

10.13.Згода не вважається добровільною, якщо надання послуги безпідставно ставиться в залежність від згоди на обробку даних, які не є необхідними для її надання.

10.14.Суб'єкт персональних даних може відкликати згоду в будь-який момент.

Відкликання згоди:

- не впливає на законність обробки, здійсненої до її відкликання;
- не припиняє обробку, якщо існує інша належна правова підстава;
- може призвести до недоступності окремої необов'язкової функції.

GDPR передбачає декілька самостійних правових підстав обробки, тому згода не є єдиною можливою підставою.

10.15. Встановлення, реалізація та захист правових вимог

Perevir може обробляти й зберігати персональні дані, якщо це необхідно для:

- підтвердження факту використання Системи;
- розгляду претензії;
- стягнення заборгованості;
- розслідування порушення;
- захисту в суді;
- виконання судового рішення;
- захисту інтелектуальної власності;
- захисту прав Користувачів або Адміністрації.

10.16. Захист життєво важливих інтересів

У виняткових випадках дані можуть оброблятися, якщо це необхідно для захисту життя, здоров'я або іншого життєво важливого інтересу фізичної особи, коли отримання згоди неможливе.

10.17. Виконання завдання в суспільному інтересі

Якщо це прямо передбачено законом, персональні дані можуть оброблятися для виконання завдання, що здійснюється в суспільному інтересі або в межах офіційних повноважень відповідного суб'єкта.

10.18. Обробка даних із державних та офіційних джерел

Правовою підставою обробки інформації з державних реєстрів та офіційних ресурсів може бути:

- прямий дозвіл закону;
- виконання договору;
- законний інтерес;
- виконання юридичного обов'язку;
- офіційне оприлюднення інформації відповідним розпорядником;
- договір інформаційної взаємодії;
- ліцензія або інша законна підстава доступу.

10.19. Perevir не вважає, що сам факт технічної доступності інформації автоматично є достатньою правовою підставою для будь-якого способу її використання.

10.20. Обробка за дорученням корпоративного Користувача

Якщо Perevir виступає розпорядником або обробником, правову підставу для обробки даних визначає корпоративний Користувач як володілець або контролер.

10.21.У такому випадку корпоративний Користувач відповідає за:

- законність мети;
- визначення правової підстави;

- дотримання прав суб’єктів;
- належне інформування;
- відповідність обсягу даних заявленій меті;
- законність рішень, прийнятих на підставі результатів Perevir.

10.22. Perevir має право відмовитися від виконання вказівки корпоративного Користувача, якщо така вказівка:

- явно суперечить закону;
- передбачає незаконний доступ до даних;
- є надмірною або дискримінаційною;
- створює неприйнятний ризик для прав суб’єктів;
- порушує правила відповідного джерела;
- суперечить Правилам користування Perevir.

10.23. Спеціальні категорії даних

Спеціальні категорії персональних даних обробляються лише за наявності спеціальної правової підстави та додаткових гарантій, передбачених застосовним законодавством.

10.24. Perevir не використовує спеціальні категорії персональних даних для маркетингу, поведінкової реклами або створення дискримінаційних профілів.

10.25. Зміна правової підстави

Якщо мета обробки істотно змінюється, Адміністрація:

- повторно оцінює правову підставу;
- перевіряє сумісність нової мети з первинною;
- за необхідності надає додаткове повідомлення;
- отримує згоду, якщо вона є обов’язковою;
- припиняє обробку, якщо належна підстава відсутня.

Нижче — проєкт розділів 10–13 у стилі попередніх частин Політики. Формулювання враховують чинний Закон України «Про захист персональних даних», Закон України «Про електронну ідентифікацію та електронні довірчі послуги», офіційні правила роботи Дія.Підпису та, де застосовується, GDPR. (Законодавство України)

11. Ідентифікація за допомогою КЕП і Дія.Підпису

11.1.Для доступу до окремих функцій Perevir Користувачеві може бути запропоновано пройти електронну ідентифікацію за допомогою:

- кваліфікованого електронного підпису;
- Дія.Підпису;
- іншого засобу електронної ідентифікації, дозволеного законодавством та підтримуваного Системою.

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» визначає правові й організаційні засади такої ідентифікації та вимагає захисту персональних даних, що обробляються під час відповідних процедур. (Законодавство України)

11.2.Електронна ідентифікація може бути необхідною для:

- підтвердження особи Користувача;
- підтвердження повноважень представника юридичної особи;
- надання доступу до окремих категорій інформації;
- виконання вимог законодавства;
- підписання заяв, договорів або інших електронних документів;
- підтвердження юридично значущої дії;
- запобігання шахрайству та несанкціонованому доступу;
- фіксації факту отримання Користувачем відповідної інформації.

11.3. Perevir може обмежити доступ до певної функції до моменту успішного проходження електронної ідентифікації.

11.4. Дані, що можуть оброблятися під час ідентифікації

Залежно від обраного засобу ідентифікації Perevir може отримувати:

- прізвище, власне ім’я та по батькові;
- РНОКПП;
- відомості про юридичну особу;
- код ЄДРПОУ;
- відомості про посаду або повноваження;
- дані кваліфікованого сертифіката відкритого ключа;
- найменування надавача електронних довірчих послуг;
- серійний номер або інший ідентифікатор сертифіката;
- строк чинності сертифіката;
- статус сертифіката;
- результат перевірки електронного підпису;
- дату й час операції;
- технічний ідентифікатор транзакції;
- інші мінімально необхідні атрибути.

11.5. Perevir обробляє лише той обсяг ідентифікаційних даних, який є необхідним для конкретної мети.

11.6. Використання КЕП

Під час використання КЕП операції створення й перевірки електронного підпису можуть здійснюватися за участю кваліфікованого надавача електронних довірчих послуг.

11.7. Perevir може перевіряти:

- чинність кваліфікованого сертифіката;
- належність сертифіката підписувачу;
- цілісність підписаних даних;
- час підписання;
- статус відкликання або блокування сертифіката;
- інші технічні атрибути, необхідні для перевірки підпису.

11.8. Perevir не зберігає:

- особистий ключ КЕП;
- пароль або код доступу до ключа;
- секретні дані створення електронного підпису;
- інші засоби, які дозволяють Адміністрації самостійно накладати підпис від імені Користувача.

Це відповідає первинній політиці Perevir, у якій прямо вказано, що приватні ключі КЕП та паролі до них не зберігаються.

11.9.Якщо Користувач самостійно завантажує файл особистого ключа до інтерфейсу зовнішнього сервісу підписання, такий файл не повинен передаватися до постійного сховища Perevir, якщо інше прямо не передбачене окремою функцією та належно не погоджене з Користувачем.

11.10. Використання Дія.Підпису

Під час використання Дія.Підпису Perevir може:

- сформувати запит на ідентифікацію або підписання;
- відобразити QR-код або інший технічний механізм запуску операції;
- перенаправити Користувача до застосунку «Дія»;
- отримати результат ідентифікації або підписання;
- отримати дозволені ідентифікаційні атрибути;
- зафіксувати дату, час і результат операції.

Офіційні матеріали Дії передбачають використання Дія.Підпису для авторизації та підписання документів у процесах організацій, які інтегрували цей механізм. (paperless.diia.gov.ua)

11.11.Активація, зберігання ключового матеріалу та підтвердження операції Дія.Підписом здійснюються у відповідній державній інфраструктурі та застосунку «Дія», а не безпосередньо в Perevir.

Офіційний центр сертифікації Дії зазначає, що в Дія.Підписі використовується роздільне безпечне зберігання особистих ключів. (ДІЯ)

11.12. Perevir не отримує:

- PIN-код Дія.Підпису;
- біометричні дані, використані застосунком «Дія»;
- зображення обличчя, зроблене для підтвердження особи в застосунку;
- особистий ключ Дія.Підпису;
- інші секретні дані, які залишаються в інфраструктурі відповідного надавача.

11.13. Самостійність постачальників ідентифікації

Кваліфіковані надавачі електронних довірчих послуг, державні інформаційні системи та застосунок «Дія» можуть самостійно визначати цілі й засоби обробки даних у межах надання власних послуг.

11.14.Обробка даних такими постачальниками здійснюється відповідно до їхнього законодавчого статусу, правил, політик конфіденційності та технічної документації.

11.15. Зберігання результатів ідентифікації

Perevir може зберігати:

- факт проходження ідентифікації;
- обраний спосіб ідентифікації;
- дату й час;
- результат операції;
- ідентифікаційні атрибути;
- технічний номер транзакції;
- відомості, необхідні для аудиту;
- електронний документ і дані перевірки підпису, якщо це необхідно для виконання договору або закону.

11.16.Строк зберігання таких відомостей визначається:

- метою операції;
- строком договірних відносин;

- строками позовної давності;
- вимогами законодавства;
- необхідністю підтвердження юридично значущої дії;
- внутрішніми правилами зберігання інформації.

11.17. Відповідальність Користувача

Користувач зобов'язаний:

- використовувати лише власний засіб електронної ідентифікації;
- не передавати ключ, пароль, PIN-код або пристрій іншій особі;
- забезпечувати конфіденційність даних доступу;
- негайно припинити використання скомпрометованого ключа;
- повідомити відповідного надавача про компрометацію;
- не використовувати сертифікат, строк чинності якого закінчився або який відкликано;
- перевіряти зміст документа перед підписанням.

11.18.Дії, підтверджені належним електронним підписом або засобом електронної ідентифікації, можуть вважатися вчиненими відповідним Користувачем, якщо відсутні обґрунтовані докази компрометації або незаконного використання.

11.19. Невдала або перервана ідентифікація

Ідентифікація може бути відхилена або не завершена, зокрема, у разі:

- помилки зовнішнього сервісу;
- недійсного чи відкликаного сертифіката;
- невідповідності даних;
- скасування операції Користувачем;
- закінчення часу сесії;
- відсутності необхідного документа;
- технічної несумісності;
- підозри на шахрайство;
- інших причин, визначених постачальником ідентифікації.

11.20.У разі невдалої ідентифікації Perevir може зберігати обмежені технічні відомості про помилку для безпеки, підтримки та діагностики.

12. Дані про використання Системи та журналювання

12.1.Під час використання Perevir автоматично формуються технічні журнали, записи подій та інші дані про взаємодію Користувача із Системою.

12.2.Журналювання здійснюється для:

- забезпечення інформаційної безпеки;
- контролю доступу;
- виявлення несанкціонованих дій;
- розслідування інцидентів;
- забезпечення стабільності;
- технічної діагностики;
- підтримки Користувачів;
- підтвердження факту виконання операцій;
- контролю дотримання Правил;
- захисту прав Адміністрації та Користувачів;
- виконання законодавчих і договірних вимог.

Загальна політика Binotel передбачає журналювання й моніторинг операцій із персональними даними для виявлення несанкціонованих або аномальних дій.

12.3. Категорії журналів

Perevir може вести:

- журнали автентифікації;
- журнали електронної ідентифікації;
- журнали доступу до функцій;
- журнали пошукових запитів;
- журнали формування та завантаження звітів;
- журнали моніторингу;
- журнали адміністративних дій;
- журнали безпеки;
- журнали API;
- журнали системних помилок;
- журнали інтеграцій;
- журнали платіжних і договірних подій;
- журнали звернень до підтримки.

12.4. Дані журналів

Залежно від типу операції журнали можуть містити:

- ідентифікатор Користувача;
- ідентифікатор корпоративного облікового запису;
- IP-адресу;
- дату й час;
- часовий пояс;
- ідентифікатор сесії;
- тип пристрою;
- браузер;

- операційну систему;
- тип виконаної дії;
- ресурс або функцію, до яких здійснювався доступ;
- параметри запиту;
- джерело інформації;
- результат операції;
- код помилки;
- обсяг переданих даних;
- ідентифікатор API-запиту;
- інформацію про зміну прав доступу;
- дані про блокування;
- інші технічні атрибути.

12.5. Perevir прагне не включати до технічних журналів:

- паролі;
- особисті ключі КЕП;
- PIN-коди;
- повні реквізити платіжних карток;
- інші секретні автентифікаційні дані.

12.6.Якщо окремі персональні дані технічно необхідні для журналювання, доступ до таких журналів обмежується, а строк їх зберігання визначається з урахуванням ризику.

12.7. Журналювання пошукових запитів

Для безпеки, аудиту й дотримання обмежень Perevir може фіксувати:

- хто здійснив запит;
- коли він був здійснений;
- який тип інформації запитувався;
- які джерела були використані;
- який результат був наданий;
- чи здійснювалося завантаження або експорт;
- чи був запит відхилений або обмежений.

12.8.Журнали пошукових запитів можуть містити персональні дані осіб, яких перевіряє Користувач, тому вони не є загальнодоступними та обробляються з обмеженим доступом.

12.9. Журналювання адміністративних дій

Perevir може фіксувати дії адміністраторів корпоративного облікового запису та уповноважених працівників Адміністрації, зокрема:

- створення або видалення Користувача;
- зміну ролі;
- зміну прав доступу;
- блокування облікового запису;
- зміну налаштувань;
- перегляд даних у межах підтримки;
- експорт;
- зміну конфігурації;
- інші привілейовані операції.

12.10.Адміністративне журналювання використовується для забезпечення підзвітності та контролю за діями осіб із підвищеними правами доступу.

12.11. Моніторинг безпеки

Perevir може автоматично аналізувати журнали для виявлення:

- великої кількості невдалих входів;
- аномальних IP-адрес;
- нетипової географії входів;
- надмірної кількості запитів;
- автоматизованого збору даних;
- спроб обходу технічних обмежень;
- підозрілих операцій;
- використання викрадених даних доступу;
- ознак атак;
- інших аномалій.

12.12.На підставі таких сигналів Perevir може:

- вимагати повторної автентифікації;
- обмежити сесію;
- тимчасово призупинити функцію;
- заблокувати обліковий запис;
- звернутися до Користувача;
- розпочати внутрішнє розслідування;
- вжити інших пропорційних заходів безпеки.

12.13.Автоматичне безпекове блокування не є рішенням щодо правового, професійного або соціального статусу Користувача, а є тимчасовим технічним заходом захисту Системи.

12.14. Доступ до журналів

Доступ до журналів може надаватися лише:

- уповноваженим працівникам Адміністрації;
- спеціалістам з інформаційної безпеки;
- технічній підтримці в необхідному обсязі;
- уповноваженим представникам корпоративного Користувача;
- аудиторам за умов конфіденційності;
- компетентним органам на підставі законної вимоги;
- іншим особам, які мають належну правову підставу.

12.15.Доступ до журналів надається за принципом найменших привілеїв і може додатково журналюватися.

12.16. Строки зберігання журналів

Журнали зберігаються протягом строку, необхідного для мети їх формування, з урахуванням:

- характеру події;
- ризику безпеки;
- строку договірних відносин;
- строків позовної давності;
- законодавчих вимог;
- необхідності розслідування інциденту;
- внутрішніх строків зберігання.

12.17.Різні категорії журналів можуть мати різні строки зберігання.

12.18.Після закінчення строку журнали:

- видаляються;
- знеособлюються;
- агрегуються;
- зберігаються довше лише за наявності окремої законної підстави.

12.19. Аналітика використання

Дані про використання Системи можуть оброблятися для:

- оцінювання навантаження;
- аналізу популярності функцій;
- виявлення помилок;
- планування ресурсів;
- оптимізації інтерфейсу;
- удосконалення продуктивності;
- формування внутрішньої статистики.

12.20.Для аналітики Perevir переважно використовує агреговані або знеособлені дані, якщо мета може бути досягнута без прямої ідентифікації Користувача.

12.21. Доказове значення журналів

Технічні журнали можуть використовуватися як доказ:

- створення облікового запису;
- входу до Системи;
- проходження ідентифікації;
- формування запиту;
- надання доступу;
- завантаження звіту;
- прийняття умов;
- виконання адміністративної дії;
- порушення Правил;
- виникнення технічного або безпекового інциденту.

12.22.Журнали не вважаються безумовним доказом вини Користувача та оцінюються разом з іншими доступними обставинами.

13. Cookies та аналогічні технології

13.1. Perevir може використовувати cookies та аналогічні технології для забезпечення функціонування вебсайту й Системи, автентифікації, безпеки, збереження налаштувань та аналізу використання.

13.2. Cookies - це невеликі файли або набори даних, які зберігаються на пристрої Користувача або зчитуються з нього під час відвідування вебсайту.

13.3.Крім cookies, Perevir може використовувати:

- local storage;
- session storage;
- технічні ідентифікатори;
- токени сесії;
- пікселі;
- серверні журнали;
- SDK;
- інші аналогічні технології.

13.4. Обов’язкові cookies

Обов’язкові cookies необхідні для роботи Perevir і можуть використовуватися для:

- створення та підтримання сесії;
- входу до облікового запису;
- захисту від підроблення запитів;
- балансування навантаження;
- збереження безпекових параметрів;
- забезпечення основної функціональності;
- запам’ятовування налаштувань конфіденційності.

13.5.Без обов’язкових cookies окремі функції Perevir можуть працювати некоректно або бути недоступними.

13.6.Обов’язкові cookies не використовуються для сторонньої рекламної поведінкової аналітики.

13.7. Cookies автентифікації

Cookies автентифікації можуть використовуватися для:

- розпізнавання активної сесії;
- збереження входу;
- перевірки належності запиту авторизованому Користувачу;
- запобігання несанкціонованому доступу;
- завершення сесії після періоду неактивності.

13.8.Токени автентифікації не повинні містити пароль Користувача у відкритому вигляді.

13.9. Функціональні cookies

Функціональні cookies можуть зберігати:

- мову інтерфейсу;
- часовий пояс;
- вибрані фільтри;
- налаштування відображення;
- стан інформаційних повідомлень;
- інші параметри персоналізації.

13.10. Аналітичні cookies

За наявності належної правової підстави Perevir може використовувати аналітичні cookies для:

- підрахунку відвідувань;
- аналізу навігації;
- оцінювання використання функцій;

- виявлення технічних проблем;
- вимірювання продуктивності;
- удосконалення інтерфейсу.

13.11.Аналітичні cookies, які не є технічно необхідними, застосовуються лише за згодою Користувача, якщо така згода вимагається застосовним законодавством.

13.12. Cookies безпеки

Cookies і технічні ідентифікатори можуть використовуватися для:

- виявлення підозрілих сесій;
- запобігання повторним атакам;
- обмеження частоти запитів;
- захисту від ботів;
- виявлення зловживань;
- підтвердження цілісності сесії;
- захисту облікового запису.

13.13. Маркетингові cookies

Perevir може використовувати маркетингові або рекламні cookies лише за наявності належної правової підстави та, якщо це необхідно, окремої згоди Користувача.

13.14.Маркетингові cookies можуть використовуватися для:

- вимірювання ефективності рекламних кампаній;
- обмеження кількості показів;
- визначення джерела переходу;
- формування аудиторій;
- персоналізації рекламних матеріалів.

13.15.Якщо Perevir фактично не використовує маркетингові cookies, цей підрозділ може бути вилучений із публічної редакції Політики.

13.16. Сторонні cookies

Окремі cookies можуть установлюватися сторонніми постачальниками, зокрема сервісами:

- вебаналітики;
- моніторингу;
- технічної підтримки;
- захисту від атак;
- платіжної інфраструктури;
- відео або іншого вбудованого контенту.

13.17.Такі постачальники можуть виступати:

- обробниками Perevir;
- самостійними контролерами;
- спільними контролерами,

залежно від характеру послуги та розподілу повноважень.

13.18.Обробка даних стороннім постачальником може додатково регулюватися його політикою конфіденційності.

13.19. Строк дії cookies

Cookies можуть бути:

- **сесійними** - видаляються після завершення сесії або закриття браузера;
- **постійними** - зберігаються протягом визначеного строку або до їх видалення Користувачем.

13.20.Строк зберігання конкретного cookie визначається його функцією, метою, налаштуваннями та застосовними вимогами законодавства.

13.21. Керування згодою

Під час першого відвідування Perevir Користувачеві може відображатися інструмент керування cookies, за допомогою якого він може:

- прийняти всі cookies;
- відхилити необов’язкові cookies;
- обрати окремі категорії;
- змінити свій вибір.

13.22.Відмова від необов’язкових cookies не повинна блокувати доступ до основної функціональності Perevir.

13.23.Користувач може змінити налаштування cookies:

- у відповідному інструменті Perevir;
- у налаштуваннях браузера;
- шляхом видалення збережених cookies;
- за допомогою інших доступних технічних засобів.

13.24.Блокування всіх cookies у браузері може призвести до:

- неможливості входу;
- завершення сесії;

- втрати налаштувань;
- неправильної роботи окремих функцій;
- необхідності повторної автентифікації.

13.25. Дані, пов’язані з cookies

Через cookies та аналогічні технології можуть оброблятися:

- IP-адреса;
- ідентифікатор сесії;
- ідентифікатор пристрою;
- тип браузера;
- операційна система;
- мова;
- дата й час;
- сторінки та функції, що використовуються;
- джерело переходу;
- технічні параметри;
- вибір Користувача щодо cookies.

13.26. Perevir не використовує cookies для зберігання:

- пароля у відкритому вигляді;
- особистого ключа КЕП;
- PIN-коду Дія.Підпису;
- повних платіжних реквізитів;
- іншої критичної секретної інформації.

13.27. Оновлення переліку cookies

Перелік cookies може змінюватися у зв’язку з:

- оновленням функціональності;
- заміною технічного постачальника;
- впровадженням нового модуля;
- зміною вимог безпеки;
- зміною законодавства.

13.28.Істотні зміни щодо необов’язкових cookies можуть супроводжуватися повторним запитом згоди.

13.29.Детальний перелік cookies із зазначенням їхньої назви, постачальника, мети, категорії та строку дії може бути опублікований в окремій **Політиці використання cookies** або в інструменті керування згодою.

14. Передавання даних постачальникам і третім особам

14.1. Perevir може передавати персональні дані постачальникам послуг, партнерам, державним органам та іншим третім особам лише:

- за наявності належної правової підстави;
- для визначеної та законної мети;
- у мінімально необхідному обсязі;
- із дотриманням вимог конфіденційності та інформаційної безпеки;
- відповідно до цієї Політики, договорів і застосовного законодавства.

Закон України «Про захист персональних даних» визначає третьою особою будь-яку особу, якій володілець або розпорядник передає персональні дані, крім самого суб'єкта, володільця, розпорядника та Уповноваженого Верховної Ради України з прав людини. (Законодавство України)

14.2.Передавання персональних даних може здійснюватися:

- шляхом надання доступу до інформаційної системи;
- через API;
- через захищені інтеграційні канали;
- шляхом надсилання електронних документів;
- через системи електронного документообігу;
- через захищені хмарні сервіси;
- в іншій законній і технічно захищеній формі.

14.3. Постачальники технічної інфраструктури

Perevir може передавати або надавати доступ до персональних даних постачальникам, які забезпечують:

- хостинг;
- хмарну інфраструктуру;
- серверні потужності;
- зберігання даних;
- резервне копіювання;
- відновлення після збоїв;
- доставку контенту;
- балансування навантаження;
- адміністрування технічної інфраструктури.

14.4. Постачальники інформаційної безпеки

Дані можуть передаватися постачальникам, які забезпечують:

- моніторинг безпеки;

- виявлення атак;
- захист від шкідливого програмного забезпечення;
- запобігання шахрайству;
- аналіз журналів;
- управління вразливостями;
- реагування на інциденти;
- захист від ботів, автоматизованого збору даних та DDoS-атак.

14.5. Постачальники електронної ідентифікації

Для забезпечення ідентифікації та перевірки електронного підпису дані можуть передаватися:

- кваліфікованим надавачам електронних довірчих послуг;
- державним інформаційним системам;
- технічним адміністраторам відповідних систем;
- застосунку «Дія» та пов’язаній державній інфраструктурі;
- іншим законним постачальникам засобів електронної ідентифікації.

14.6.Таким постачальникам передається лише інформація, необхідна для:

- формування запиту на ідентифікацію;
- перевірки сертифіката;
- перевірки електронного підпису;
- підтвердження особи;
- підтвердження повноважень;
- отримання результату операції.

14.7. Постачальники інформаційних даних

Для надання функціональності Perevir інформація може передаватися або отримуватися через:

- державні реєстри;
- офіційні інформаційні системи;
- портали відкритих даних;
- ліцензовані інформаційні платформи;
- комерційні бази даних;
- партнерські API;
- інші законні джерела.

14.8.Під час звернення до зовнішнього інформаційного джерела Perevir може передавати:

- пошуковий критерій;

- код ЄДРПОУ;
- ПІБ;
- РНОКПП, якщо його використання дозволене;
- номер справи або провадження;
- технічний ідентифікатор запиту;
- інші мінімально необхідні параметри.

14.9.Конкретний обсяг даних залежить від:

- функції, яку використовує Користувач;
- технічних вимог інтеграції;
- режиму доступу до джерела;
- умов договору з постачальником;
- вимог законодавства.

14.10. Платіжні постачальники

Для здійснення оплати та обліку платежів дані можуть передаватися:

- банкам;
- платіжним установам;
- еквайринговим сервісам;
- платіжним системам;
- бухгалтерам;
- аудиторам;
- іншим постачальникам фінансових послуг.

14.11. Perevir передає таким особам лише дані, необхідні для:

- проведення платежу;
- підтвердження транзакції;
- виставлення рахунку;
- повернення коштів;
- бухгалтерського обліку;
- податкової звітності;
- запобігання платіжному шахрайству.

14.12.Повні реквізити платіжної картки можуть оброблятися безпосередньо банком або платіжним провайдером і не повинні передаватися до Perevir, якщо інше прямо не передбачено обраним способом оплати.

14.13. Постачальники комунікацій

Контактні та технічні дані можуть передаватися постачальникам:

- електронної пошти;

- SMS-повідомлень;
- сервісних сповіщень;
- push-повідомлень;
- служби підтримки;
- систем управління зверненнями;
- корпоративних комунікаційних платформ.

14.14. Постачальники аналітики та моніторингу

За наявності належної правової підстави технічні дані можуть передаватися постачальникам:

- вебаналітики;
- моніторингу продуктивності;
- діагностики помилок;
- аналізу доступності;
- оцінювання використання функцій;
- технічної статистики.

14.15.Для такої обробки Perevir, наскільки це технічно можливо, використовує:

- псевдонімізацію;
- скорочення IP-адрес;
- мінімізацію параметрів;
- обмеження строків зберігання;
- відключення необов’язкового відстеження;
- агреговані або знеособлені дані.

14.16. Професійні консультанти

Персональні дані можуть передаватися в необхідному обсязі:

- адвокатам;
- юридичним радникам;
- аудиторам;
- бухгалтерам;
- податковим консультантам;
- страховикам;
- спеціалістам з інформаційної безпеки;
- іншим професійним консультантам.

Таке передавання може здійснюватися для:

- отримання професійної консультації;
- проведення аудиту;
- виконання законодавчих вимог;

- захисту прав;
- розгляду спорів;
- розслідування інцидентів.

14.17. Передавання корпоративному Користувачу

Якщо обліковий запис належить корпоративному Користувачу, уповноваженим адміністраторам такого облікового запису можуть бути доступні:

- дані профілю Користувача;
- статус облікового запису;
- роль і права доступу;
- історія входів;
- історія використання корпоративної функціональності;
- сформовані звіти;
- налаштування моніторингу;
- інші дані в межах корпоративного середовища.

14.18.Корпоративний Користувач самостійно відповідає за:

- визначення кола уповноважених адміністраторів;
- законність внутрішнього контролю;
- інформування своїх працівників;
- належне використання отриманої інформації;
- захист даних після їх отримання.

14.19. Передавання за згодою або за вказівкою Користувача

Perevir може передавати дані третій особі, якщо Користувач:

- прямо доручив здійснити таке передавання;
- активував відповідну інтеграцію;
- експортував звіт;
- надав доступ іншому Користувачу;
- погодив передавання в межах окремої функції;
- надав належну згоду, якщо вона необхідна.

14.20.До активації зовнішньої інтеграції Користувач повинен перевірити:

- хто є одержувачем даних;
- які дані передаватимуться;
- для якої мети;
- у якій країні вони оброблятимуться;
- які правила конфіденційності застосовуються.

14.21. Передавання державним органам

Perevir може передавати персональні дані:

- судам;
- правоохоронним органам;
- органам державної влади;
- органам місцевого самоврядування;
- контролюючим і регуляторним органам;
- державним виконавцям;
- іншим уповноваженим суб’єктам,

якщо таке передавання вимагається або дозволяється законом.

14.22.До надання інформації за запитом компетентного органу Perevir може перевіряти:

- повноваження запитувача;
- законну підставу запиту;
- форму та зміст документа;
- обсяг запитуваних даних;
- співмірність запиту;
- наявність законних обмежень щодо розкриття.

14.23. Perevir може відмовити в передаванні або вимагати уточнення запиту, якщо:

- запит поданий неналежною особою;
- відсутня правова підстава;
- запит не відповідає встановленій формі;
- обсяг даних є явно надмірним;
- передавання заборонене законом;
- запит не дозволяє однозначно визначити необхідну інформацію.

14.24. Передавання у зв’язку з корпоративними змінами

Персональні дані можуть бути передані потенційному або фактичному правонаступнику у зв’язку з:

- реорганізацією;
- злиттям;
- приєднанням;
- поділом;
- перетворенням;
- продажем бізнесу або активів;
- передаванням прав на Perevir;
- залученням інвестора;
- процедурою банкрутства.

14.25.До завершення такої операції доступ до персональних даних повинен обмежуватися мінімально необхідним обсягом і надаватися на умовах конфіденційності.

14.26. Вимоги до постачальників

До залучення постачальника Perevir може оцінювати:

- характер послуг;
- категорії даних;
- ризик для прав суб’єктів;
- місце обробки;
- технічні та організаційні заходи;
- практики реагування на інциденти;
- умови залучення субпостачальників;
- строки зберігання;
- порядок повернення та видалення даних.

14.27.Якщо постачальник обробляє дані від імені Perevir, відповідні відносини оформлюються договором або іншим юридично обов’язковим документом.

Такий документ може визначати:

- предмет та строк обробки;
- характер і мету операцій;
- категорії персональних даних;
- категорії суб’єктів;
- вимоги конфіденційності;
- заходи безпеки;
- порядок залучення субпроцесорів;
- допомогу у виконанні прав суб’єктів;
- порядок повідомлення про інциденти;
- умови повернення та видалення інформації.

За GDPR обробник повинен діяти на підставі договору або іншого обов’язкового документа, який визначає предмет, строк, характер, мету обробки та обов’язки сторін. (EUR-Lex)

14.28. Perevir не надає постачальникам право:

- використовувати дані для несумісних цілей;
- продавати дані;
- формувати незалежні маркетингові профілі без правової підстави;
- передавати дані невизначеному колу осіб;
- зберігати дані довше, ніж це необхідно.

14.29.Окремий постачальник може виступати самостійним володільцем або контролером, якщо він сам визначає мету та істотні засоби обробки, зокрема під час:

- надання платіжних послуг;
- виконання власних юридичних обов'язків;
- надання кваліфікованих електронних довірчих послуг;
- ведення державного реєстру;
- здійснення власної професійної діяльності.

14.30. Perevir не продає персональні дані Користувачів третім особам і не передає їх для незалежного рекламного використання без належної правової підстави.

14.31.Перелік категорій постачальників може змінюватися разом із розвитком Perevir. Інформація про істотні зміни, які впливають на права суб'єктів даних, може надаватися шляхом оновлення цієї Політики, окремого повідомлення або інструменту керування згодою.

15. Міжнародне передавання персональних даних

15.1.У процесі використання Perevir персональні дані можуть передаватися або ставати доступними одержувачам, серверам чи технічним постачальникам, розташованим за межами України.

15.2.Міжнародне передавання може відбуватися, зокрема, у зв'язку з використанням:

- хмарної інфраструктури;
- резервного копіювання;
- сервісів електронної пошти;
- систем аналітики;
- засобів моніторингу та кібербезпеки;
- міжнародних платіжних сервісів;
- систем технічної підтримки;
- зовнішніх API;
- корпоративних сервісів міжнародної групи компаній;
- інших постачальників із транскордонною інфраструктурою.

15.3.Сам факт того, що постачальник зареєстрований в Україні або Європейському Союзі, не виключає можливості обробки інформації в інших державах через його сервери, субпроцесорів або служби підтримки.

15.4.Перед міжнародним передаванням Perevir визначає:

- країну призначення;
- категорії одержувачів;

- мету передавання;
- категорії даних;
- правову підставу;
- рівень захисту в державі призначення;
- наявні договірні та технічні гарантії;
- ризики доступу з боку іноземних органів;
- можливість застосування додаткових заходів.

15.5. Передавання відповідно до законодавства України

Міжнародне передавання персональних даних здійснюється відповідно до вимог Закону України «Про захист персональних даних», міжнародних договорів України та інших застосовних нормативно-правових актів.

15.6.Передавання іноземному суб'єкту може здійснюватися, якщо:

- відповідна держава забезпечує належний захист персональних даних;
- передавання дозволене законом або міжнародним договором;
- суб'єкт надав однозначну згоду, якщо вона є належною підставою;
- передавання необхідне для укладення або виконання договору;
- передавання необхідне для захисту життєво важливих інтересів;
- передавання необхідне для встановлення, реалізації або захисту правових вимог;
- існує інша належна правова підстава.

Українські нормативні акти у сфері обробки персональних даних передбачають, що передавання іноземним суб'єктам має здійснюватися з урахуванням належного рівня захисту та вимог закону або міжнародного договору. (Законодавство України)

15.7. Передавання відповідно до GDPR

Якщо до конкретної операції застосовується GDPR, передавання персональних даних за межі Європейської економічної зони здійснюється відповідно до глави V GDPR.

15.8.Таке передавання може ґрунтуватися, зокрема, на:

- рішенні Європейської Комісії про належний рівень захисту;
- стандартних договірних положеннях;
- обов'язкових корпоративних правилах;
- затвердженому кодексі поведінки;
- механізмі сертифікації;
- спеціальному винятку, передбаченому GDPR.

Правила GDPR щодо міжнародного передавання спрямовані на те, щоб рівень захисту фізичних осіб не знижувався внаслідок переміщення даних до третьої країни або міжнародної організації. (EUR-Lex)

15.9. Рішення про належний рівень захисту

Якщо Європейська Комісія визнала, що країна, територія або певний сектор забезпечує належний рівень захисту, передавання може здійснюватися на підставі такого рішення без окремого дозволу.

15.10. Perevir перевіряє актуальність відповідного рішення на момент організації передавання.

15.11. Стандартні договірні положення

За відсутності рішення про належний рівень захисту Perevir може використовувати стандартні договірні положення, затверджені Європейською Комісією, або інший передбачений законом механізм.

15.12.У відповідному договорі можуть визначатися:

- цілі передавання;
- категорії даних;
- категорії суб'єктів;
- одержувачі;
- строки зберігання;
- технічні та організаційні заходи;
- порядок залучення субпроцесорів;
- права суб'єктів;
- порядок повідомлення про інциденти;
- умови припинення передавання.

15.13. Оцінювання впливу передавання

Перед використанням договірного механізму Perevir може оцінювати:

- законодавство країни одержувача;
- практику доступу державних органів;
- можливість виконання договірних гарантій;
- характер і чутливість даних;
- цілі та регулярність передавання;
- можливість шифрування або псевдонімізації;
- ризик для прав і свобод суб'єктів.

15.14.За результатами оцінювання можуть застосовуватися додаткові заходи, зокрема:

- наскрізне шифрування;
- шифрування під час передавання і зберігання;
- псевдонімізація;
- поділ наборів даних;

- скорочення ідентифікаторів;
- зберігання ключів шифрування в іншій юрисдикції;
- обмеження віддаленого доступу;
- додаткові договірні зобов’язання;
- посилений аудит постачальника.

15.15. Виняткові підстави

У виняткових випадках міжнародне передавання може здійснюватися на підставі:

- однозначної поінформованої згоди;
- необхідності виконання договору із суб’єктом;
- необхідності укладення або виконання договору в інтересах суб’єкта;
- важливих підстав суспільного інтересу;
- встановлення, реалізації або захисту правових вимог;
- захисту життєво важливих інтересів;
- іншої передбаченої законом підстави.

15.16.Виняткова підстава не повинна використовуватися для систематичного та масового міжнародного передавання, якщо для такого передавання необхідний стабільний механізм захисту.

15.17. Віддалений доступ як міжнародне передавання

Надання доступу до персональних даних працівнику, підряднику або службі підтримки, які перебувають в іншій державі, може вважатися міжнародним передаванням, навіть якщо сервер фізично розташований в Україні або Європейському Союзі.

15.18. Субпроцесори

Постачальник може залучати субпроцесорів в інших країнах лише відповідно до:

- договору з Perevir;
- вимог застосовного законодавства;
- установленого механізму міжнародного передавання;
- обов’язку забезпечити не нижчий рівень захисту.

15.19. Perevir може вимагати від постачальника:

- повідомляти про нових субпроцесорів;
- зазначати країни обробки;
- забезпечувати право на заперечення;
- надавати інформацію про механізми передавання;
- підтверджувати застосування заходів безпеки.

15.20. Вимоги іноземних органів

Якщо іноземний державний орган звертається з вимогою про доступ до персональних даних, Perevir або відповідний постачальник повинні, наскільки це дозволено законом:

- перевірити законність вимоги;
- оцінити компетенцію органу;
- оскаржити явно незаконну або надмірну вимогу;
- надати мінімально необхідний обсяг даних;
- документувати розкриття;
- повідомити Perevir або суб'єкта, якщо це не заборонено законом.

15.21. Інформування суб'єктів

Інформація про міжнародне передавання може надаватися через:

- цю Політику;
- повідомлення під час збирання даних;
- договір;
- Data Processing Agreement;
- перелік постачальників;
- інструмент керування cookies;
- відповідь на запит суб'єкта.

15.22.На запит суб'єкта Perevir може надати загальну інформацію про:

- категорії країн призначення;
- категорії одержувачів;
- правову підставу;
- застосовані гарантії;
- спосіб отримання копії або опису відповідного механізму, якщо це дозволено законом і договором.

16. Строки зберігання та видалення персональних даних

16.1. Perevir зберігає персональні дані лише протягом строку, необхідного для досягнення мети їх обробки, якщо довший строк не вимагається або не дозволяється законодавством.

Принцип обмеження строку зберігання передбачає, що дані повинні зберігатися у формі, яка дозволяє ідентифікацію особи, не довше, ніж це потрібно для відповідної мети. (EUR-Lex)

16.2.Під час визначення строку зберігання Perevir враховує:

- мету обробки;
- правову підставу;
- характер і обсяг даних;
- договірні відносини;
- вимоги законодавства;
- строки позовної давності;
- потребу у виконанні правових вимог;
- ризик для прав і свобод суб'єктів;
- строки, установлені відповідним реєстром або постачальником;
- необхідність забезпечення інформаційної безпеки;
- технічні цикли резервного копіювання.

16.3.Строки зберігання можуть визначатися:

- цією Політикою;
- внутрішнім графіком зберігання;
- договором із Користувачем;
- Data Processing Agreement;
- умовами відповідної функції;
- нормативно-правовим актом;
- згодою суб'єкта;
- правилами зовнішнього джерела.

Типовий порядок обробки персональних даних вимагає, щоб володілець визначив строк та умови зберігання, а також процедуру зміни, видалення або знищення даних. (Законодавство України)

16.4. Дані облікового запису

Дані облікового запису можуть зберігатися:

- протягом строку його активності;
- протягом строку дії договору;
- після закриття облікового запису — протягом періоду, необхідного для завершення розрахунків, розгляду претензій, захисту прав та виконання законодавчих вимог.

16.5.Після закриття облікового запису Perevir може:

- видалити дані;
- знеособити їх;
- обмежити обробку;
- перемістити їх до архівного середовища з обмеженим доступом;
- зберегти окремі відомості на підставі закону або законного інтересу.

16.6. Дані договорів і розрахунків

Договори, рахунки, акти, платіжні та бухгалтерські документи зберігаються протягом строків, установлених:

- податковим законодавством;
- бухгалтерськими правилами;
- архівними вимогами;
- строками позовної давності;
- іншими обов'язковими нормами.

16.7.Закриття облікового запису або відкликання згоди не є підставою для дострокового знищення документів, які Perevir зобов'язаний зберігати відповідно до закону.

16.8. Дані електронної ідентифікації

Відомості про електронну ідентифікацію можуть зберігатися протягом строку, необхідного для:

- підтвердження факту ідентифікації;
- підтвердження юридично значущої дії;
- перевірки електронного підпису;
- виконання договору;
- розгляду спору;
- аудиту;
- виконання законодавчих вимог.

16.9. Perevir не зберігає особисті ключі КЕП, PIN-коди Дія.Підпису чи інші секретні засоби створення електронного підпису.

16.10. Історія пошукових запитів і звітів

Історія запитів, сформовані звіти та результати перевірок можуть зберігатися:

- протягом строку дії облікового запису;
- протягом строку, установленого тарифом;
- до їх видалення Користувачем;
- протягом строку, визначеного корпоративним Користувачем;
- довше - якщо це необхідно для безпеки, аудиту, спору або виконання закону.

16.11.Після видалення звіту з інтерфейсу його копія може тимчасово залишатися:

- у резервній копії;
- у журналі операцій;
- в архіві безпеки;
- у доказовому наборі, пов’язаному зі спором або інцидентом.

16.12. Дані моніторингу

Дані суб’єктів моніторингу можуть зберігатися:

- до видалення Користувачем із моніторингу;
- до закриття відповідного облікового запису;
- до припинення договору;
- протягом додаткового періоду, необхідного для завершення повідомлень, розгляду спорів або аудиту.

16.13. Дані звернень до підтримки

Звернення, листування та вкладення можуть зберігатися протягом строку, необхідного для:

- вирішення питання;
- контролю якості;
- навчання працівників із належним захистом;
- підтвердження наданої консультації;
- захисту прав сторін;
- виконання договору.

16.14. Технічні журнали

Строк зберігання журналів визначається залежно від їхнього типу.

Зокрема:

- операційні журнали можуть зберігатися протягом короткого технічного періоду;
- журнали автентифікації - протягом строку, необхідного для контролю доступу;
- журнали безпеки - протягом строку, достатнього для виявлення та розслідування інцидентів;
- журнали юридично значущих дій - протягом строку, необхідного для доказування;
- журнали інцидентів - до завершення розслідування та пов’язаних процедур.

16.15. Cookies

Строк зберігання cookies визначається їхньою категорією:

- сесійні cookies видаляються після завершення сесії;
- постійні cookies зберігаються до закінчення встановленого строку;
- необов’язкові cookies можуть бути видалені після відкликання згоди;
- безпекові cookies можуть зберігатися протягом періоду, необхідного для запобігання повторним загрозам.

16.16. Маркетингові дані

Контактні дані для маркетингових повідомлень можуть зберігатися:

- до відкликання згоди;
- до реалізації права на заперечення;
- до завершення відповідної маркетингової кампанії;
- до втрати актуальності контактних даних;
- протягом іншого законно визначеного строку.

16.17.Після відмови від розсилки Perevir може зберегти мінімальний запис про відмову, щоб не надсилати повідомлення повторно.

16.18. Дані кандидатів, представників і контактних осіб

Якщо Perevir отримує дані контактних осіб, представників або кандидатів, вони зберігаються протягом строку:

- відповідних переговорів;
- дії договору;
- виконання повноважень представника;
- розгляду кандидатури;
- іншої конкретної мети.

16.19. Дані із зовнішніх реєстрів

Інформація, отримана з державних та інших зовнішніх джерел, може:

- відображатися в актуальному стані;
- кешуватися на обмежений строк;
- зберігатися у сформованому звіті;
- архівуватися для відображення історії змін;
- оновлюватися під час наступного звернення до джерела.

16.20.Строк зберігання такої інформації залежить від:

- режиму джерела;
- договірних умов;
- технічної архітектури;
- мети звіту;

- необхідності відображення історії;
- законодавчих обмежень.

16.21.Видалення інформації з Perevir не означає її видалення з державного реєстру, офіційного джерела або системи стороннього постачальника.

16.22.Для виправлення або видалення первинної реєстрової інформації суб'єкту може бути необхідно звернутися до відповідного держателя, адміністратора або органу, який вніс такі відомості.

16.23. Резервні копії

Після видалення даних з активних систем окремі копії можуть протягом обмеженого часу залишатися в резервних копіях.

16.24.Резервні копії:

- зберігаються з обмеженим доступом;
- використовуються для відновлення після збою;
- не повинні використовуватися для звичайних операцій;
- видаляються або перезаписуються відповідно до циклу резервного копіювання;
- відновлюються лише за обґрунтованої необхідності.

16.25.Якщо резервна копія відновлюється, Perevir вживає заходів для повторного видалення даних, які до моменту відновлення вже підлягали видаленню, наскільки це технічно можливо.

16.26. Обмеження обробки замість видалення

Perevir може не видаляти дані негайно, а обмежити їх обробку, якщо:

- суб'єкт оскаржує точність інформації;
- необхідно перевірити законність обробки;
- дані потрібні для правових вимог;
- закон забороняє їх знищення;
- триває розгляд звернення або спору;
- видалення може перешкодити розслідуванню інциденту.

16.27.Під час обмеження обробки дані можуть зберігатися, але не використовуються для інших цілей, крім:

- захисту прав;
- виконання закону;
- забезпечення безпеки;
- інших передбачених законом випадків.

16.28. Підстави для видалення або знищення

Персональні дані можуть бути видалені або знищені у разі:

- закінчення строку зберігання;
- досягнення мети обробки;
- припинення правової підстави;
- відкликання згоди за відсутності іншої підстави;
- задоволення обґрунтованої вимоги суб’єкта;
- визнання обробки незаконною;
- припинення договору;
- ліквідації володільця, якщо немає правонаступника;
- іншої передбаченої законом обставини.

Законодавство України передбачає видалення або знищення даних, зокрема, після закінчення строку їх зберігання або припинення законної підстави обробки. (Законодавство України)

16.29. Способи видалення

Видалення або знищення може здійснюватися шляхом:

- логічного видалення з активної системи;
- фізичного стирання;
- криптографічного знищення ключа;
- безповоротного перезапису;
- знищення матеріального носія;
- знеособлення;
- іншого способу, що виключає подальше використання для ідентифікації.

16.30.Знищення має здійснюватися у спосіб, який виключає подальше відновлення персональних даних, якщо технічні та правові умови дозволяють остаточне знищення. (Законодавство України)

16.31. Знеособлення

Замість видалення Perevir може знеособити дані, якщо:

- вони потрібні для статистики;
- вони використовуються для дослідження продуктивності;
- вони необхідні для планування ресурсів;
- мету можна досягти без ідентифікації особи.

16.32.Після належного незворотного знеособлення інформація більше не вважається персональними даними, якщо особу неможливо ідентифікувати доступними та розумно ймовірними засобами.

16.33. Видалення за запитом суб’єкта

Суб’єкт може звернутися із запитом про видалення своїх персональних даних.

Перед виконанням запиту Perevir може:

- перевірити особу заявника;
- уточнити обсяг запиту;
- визначити роль Perevir;
- перевірити наявність іншої правової підстави;
- перевірити законодавчі строки зберігання;
- звернутися до корпоративного Користувача, якщо він є контролером відповідної обробки.

16.34. Perevir може відмовити в повному або частковому видаленні, якщо дані необхідні для:

- виконання юридичного обов’язку;
- здійснення права на свободу вираження та інформацію;
- виконання завдання в суспільному інтересі;
- встановлення, реалізації або захисту правових вимог;
- запобігання шахрайству;
- забезпечення інформаційної безпеки;
- збереження обов’язкових фінансових або договірних документів;
- іншої законної мети.

16.35.Якщо Perevir не може виконати вимогу повністю, заявнику надається пояснення в межах, передбачених законодавством.

16.36. Видалення корпоративних даних

Якщо Perevir виступає обробником, видалення або повернення даних корпоративного Користувача здійснюється:

- за його документованою вказівкою;
- після завершення договору;
- відповідно до Data Processing Agreement;
- з урахуванням законодавчих обов’язків Perevir.

16.37.Корпоративний Користувач відповідає за визначення строків зберігання даних, які він обробляє як самостійний володілець або контролер.

16.38. Періодичний перегляд

Perevir може періодично переглядати:

- категорії даних;
- строки зберігання;
- наявність правової підстави;
- активність облікових записів;
- необхідність подальшого зберігання;
- можливість знеособлення або видалення.

16.39.Неактивні облікові записи та застарілі набори даних можуть бути:

- позначені як неактивні;
- архівовані;
- обмежені;
- знеособлені;
- видалені після попереднього повідомлення, якщо воно є доцільним.

16.40.Конкретні строки для окремих категорій даних можуть визначатися у внутрішньому **Графіку зберігання та видалення даних**, який переглядається з урахуванням змін законодавства, функціональності Perevir та ризиків обробки.

17. Інформаційна безпека

17.1. Perevir вживає належних технічних та організаційних заходів для захисту персональних даних від:

- випадкової втрати або знищення;
- незаконного знищення;
- несанкціонованого доступу;
- неправомірної зміни;
- несанкціонованого копіювання;
- незаконного передавання або поширення;
- блокування;
- пошкодження;
- втрати доступності;
- інших незаконних або несанкціонованих операцій.

Закон України «Про захист персональних даних» покладає обов’язок забезпечувати захист персональних даних від випадкової втрати, знищення та незаконної обробки на володільців, розпорядників і третіх осіб. (Законодавство України)

17.2.Заходи інформаційної безпеки визначаються з урахуванням:

- характеру та обсягу персональних даних;
- цілей і способів обробки;

- категорій суб’єктів персональних даних;
- джерел отримання інформації;
- рівня конфіденційності;
- ризиків для прав і свобод фізичних осіб;
- імовірності та тяжкості можливих наслідків;
- актуального стану технологій;
- вартості та пропорційності впровадження заходів;
- договірних і законодавчих вимог.

17.3. Perevir застосовує ризик-орієнтований підхід до інформаційної безпеки та періодично переглядає заходи захисту з урахуванням:

- змін функціональності Системи;
- появи нових загроз;
- виявлених вразливостей;
- результатів аудитів і тестувань;
- змін у складі постачальників;
- змін законодавства;
- результатів розслідування інцидентів.

17.4. Управління доступом

Доступ до персональних даних надається лише особам, яким він необхідний для виконання службових, договірних або законодавчих обов’язків.

17.5.Під час надання доступу Perevir може застосовувати:

- іменні облікові записи;
- рольову модель доступу;
- принцип найменших привілеїв;
- розподіл адміністративних повноважень;
- періодичний перегляд прав доступу;
- автоматичне завершення сесій;
- блокування неактивних або скомпрометованих облікових записів;
- обмеження доступу до окремих функцій та категорій інформації;
- додаткову перевірку особи для критичних операцій.

17.6.Права доступу переглядаються, зокрема, у разі:

- зміни посади або функцій працівника;
- зміни ролі Користувача;
- припинення трудових або договірних відносин;
- переведення до іншого підрозділу;
- виявлення підозрілої активності;
- завершення відповідного проєкту;

- зміни повноважень корпоративного Користувача.

17.7.Доступ працівника, підрядника або іншої уповноваженої особи припиняється або коригується без необґрунтованої затримки після припинення потреби в такому доступі.

17.8. Автентифікація Користувачів

Для захисту облікових записів Perevir може застосовувати:

- вимоги до складності пароля;
- криптографічне перетворення паролів;
- обмеження кількості невдалих спроб входу;
- тимчасове блокування;
- безпечне відновлення доступу;
- контроль активних сесій;
- повідомлення про підозрілі входи;
- повторну автентифікацію перед критичними операціями;
- електронну ідентифікацію за допомогою КЕП, Дія.Підпису або іншого дозволеного засобу.

17.9.Паролі не повинні зберігатися у відкритому вигляді.

17.10. Perevir не отримує і не зберігає:

- особисті ключі КЕП;
- паролі до особистих ключів;
- PIN-коди Дія.Підпису;
- біометричні дані, які використовуються застосунком «Дія»;
- інші секретні засоби створення електронного підпису.

17.11. Криптографічний захист

Залежно від характеру операції Perevir може використовувати:

- шифрування даних під час передавання;
- шифрування окремих даних під час зберігання;
- захищені мережеві протоколи;
- керування криптографічними ключами;
- цифрові сертифікати;
- контроль цілісності;
- криптографічний захист резервних копій;
- інші засоби захисту інформації.

17.12.Криптографічні ключі та секрети доступу повинні:

- зберігатися окремо від даних, які вони захищають, якщо це технічно доцільно;

- бути доступними лише уповноваженим процесам та особам;
- періодично замінюватися;
- відкликатися у разі компрометації;
- не включатися до відкритого програмного коду або загальнодоступної документації.

17.13. Захист інфраструктури

Perevir може застосовувати такі заходи захисту інфраструктури:

- сегментацію мережі;
- міжмережеві екрани;
- системи виявлення та запобігання вторгненням;
- захист від DDoS-атак;
- захист від шкідливого програмного забезпечення;
- контроль конфігурацій;
- обмеження адміністративного доступу;
- моніторинг мережевої активності;
- централізоване керування журналами;
- резервування критичних компонентів;
- контроль доступності сервісів.

17.14. Управління вразливостями

Perevir може здійснювати:

- сканування вразливостей;
- аналіз залежностей і програмних компонентів;
- установлення оновлень безпеки;
- тестування захищеності;
- аналіз конфігурацій;
- контроль відомих вразливостей;
- пріоритизацію виправлень залежно від ризику;
- повторну перевірку після усунення недоліків.

17.15.Строк усунення вразливості визначається з урахуванням:

- її критичності;
- можливості експлуатації;
- доступності вразливого компонента з мережі;
- категорій даних, яких вона стосується;
- наявності тимчасових компенсуючих заходів;
- потенційного впливу на Користувачів.

17.16. Безпечна розробка та зміни

Під час розроблення й оновлення Perevir можуть застосовуватися:

- розмежування середовищ розробки, тестування та експлуатації;
- перевірка програмного коду;
- тестування змін;
- контроль доступу до репозиторіїв;
- управління залежностями;
- заборона використання реальних персональних даних у тестуванні без необхідності;
- використання знеособлених, псевдонімізованих або синтетичних тестових даних;
- контроль випуску оновлень;
- можливість відновлення попередньої стабільної версії.

17.17.Реальні персональні дані можуть використовуватися для тестування лише тоді, коли:

- мета не може бути обґрунтовано досягнута іншим способом;
- існує належна правова підстава;
- використовується мінімально необхідний обсяг;
- застосовані додаткові заходи захисту;
- доступ до тестового середовища обмежений.

17.18. Мінімізація і розмежування даних

Perevir може застосовувати:

- мінімізацію обсягу даних;
- псевдонімізацію;
- знеособлення;
- логічне розмежування клієнтських середовищ;
- окреме зберігання ідентифікаторів;
- маскування інформації в інтерфейсі;
- приховування частини значень;
- обмеження експорту;
- контроль масового завантаження.

17.19.Дані різних корпоративних Користувачів повинні бути логічно або фізично розмежовані так, щоб один Користувач не отримував несанкціонований доступ до даних іншого.

17.20. Журналювання і моніторинг

Perevir може журналювати:

- входи до облікових записів;
- невдалі спроби автентифікації;
- дії з підвищеними правами;
- зміну ролей і дозволів;
- доступ до окремих категорій інформації;
- формування та експорт звітів;
- дії через API;
- зміни конфігурацій;
- події інформаційної безпеки.

17.21.Журнали можуть автоматично аналізуватися для виявлення:

- аномальної активності;
- надмірної кількості запитів;
- автоматизованого збору інформації;
- спроб обходу обмежень;
- нетипових входів;
- ознак компрометації;
- неправомірного використання адміністративних прав;
- інших потенційних загроз.

17.22. Резервне копіювання та відновлення

Для забезпечення доступності й цілісності даних Perevir може застосовувати:

- регулярне резервне копіювання;
- захищене зберігання резервних копій;
- розмежування доступу до копій;
- періодичну перевірку можливості відновлення;
- географічне або логічне резервування;
- плани аварійного відновлення;
- процедури забезпечення безперервності діяльності.

17.23.Резервні копії використовуються лише для:

- відновлення після технічного збою;
- ліквідації наслідків інциденту;
- забезпечення безперервності роботи;
- інших визначених і законних цілей.

17.24. Фізична безпека

Якщо Perevir використовує власні або орендовані фізичні приміщення чи обладнання, можуть застосовуватися:

- контроль фізичного доступу;
- облік відвідувачів;
- відеоспостереження в дозволених законом випадках;
- захист серверного обладнання;
- протипожежні засоби;
- резервне електроживлення;
- контроль температури та інших параметрів середовища;
- безпечне знищення носіїв.

17.25. Персонал і конфіденційність

Працівники, підрядники та інші уповноважені особи, які мають доступ до персональних даних:

- зобов’язані дотримуватися конфіденційності;
- проходять інструктаж або навчання;
- отримують доступ лише в межах своїх повноважень;
- несуть відповідальність за порушення внутрішніх правил;
- повинні повідомляти про підозрювані інциденти та вразливості;
- не мають права використовувати дані у власних цілях.

17.26.Обов’язок конфіденційності може продовжувати діяти після припинення трудових або договірних відносин.

17.27. Безпека постачальників

До залучення постачальника Perevir може оцінювати:

- заходи інформаційної безпеки;
- місце обробки даних;
- умови доступу;
- практики резервного копіювання;
- порядок реагування на інциденти;
- залучення субпроцесорів;
- наявність аудитів або сертифікацій;
- порядок повернення і видалення даних.

17.28.Договори з постачальниками можуть передбачати:

- обов’язок конфіденційності;
- визначені заходи безпеки;
- обмеження цілей обробки;
- повідомлення про порушення безпеки;
- допомогу в розслідуванні;
- правила залучення субпроцесорів;

- повернення або видалення даних після завершення послуг;
- право на отримання підтверджень або проведення перевірки.

17.29. Аудити та перевірки

Perevir може проводити або замовляти:

- внутрішні аудити;
- зовнішні аудити;
- перевірки контролів доступу;
- аналіз ризиків;
- тестування на проникнення;
- перевірки конфігурацій;
- аналіз процесів реагування на інциденти;
- перевірки постачальників.

17.30.Результати аудитів використовуються для:

- усунення недоліків;
- удосконалення заходів захисту;
- актуалізації внутрішніх політик;
- навчання персоналу;
- перегляду ризиків;
- планування технічних змін.

17.31. Відповідальність Користувача

Користувач відповідає за безпеку власного доступу до Perevir та зобов’язаний:

- використовувати надійний пароль;
- не використовувати один пароль у декількох сервісах;
- не передавати дані доступу іншим особам;
- завершувати сесію на спільних пристроях;
- підтримувати актуальність програмного забезпечення;
- не обходити заходи безпеки;
- не запускати автоматизовані засоби без дозволу;
- негайно повідомляти про підозру щодо компрометації;
- перевіряти адреси електронних повідомлень і сторінок входу;
- забезпечувати безпеку власного пристрою та мережі.

17.32.Корпоративний Користувач додатково відповідає за:

- призначення адміністраторів;
- установлення внутрішніх ролей;
- своєчасне блокування звільнених працівників;

- законність внутрішнього доступу;
- захист експортованих звітів;
- безпеку власних API-ключів та інтеграцій;
- контроль за діями своїх Користувачів.

17.33.Жодна інформаційна система не може гарантувати абсолютну захищеність від усіх можливих загроз.

Водночас Perevir зобов'язується підтримувати рівень захисту, співмірний із характером обробки, доступними технологіями та встановленими ризиками.

17.34.Інформація про конкретні налаштування безпеки, схеми мережі, засоби виявлення атак, криптографічні ключі та інші деталі, розкриття яких може створити загрозу, не публікується у цій Політиці.

18. Реагування на порушення безпеки персональних даних

18.1.Порушенням безпеки персональних даних вважається подія, що призвела або могла призвести до:

- випадкового чи незаконного знищення даних;
- втрати даних;
- зміни даних;
- несанкціонованого розкриття;
- незаконного передавання;
- несанкціонованого доступу;
- втрати доступності;
- іншого порушення конфіденційності, цілісності або доступності персональних даних.

18.2.До можливих порушень можуть належати:

- компрометація облікового запису;
- викрадення пароля або токена;
- помилкове надсилання звіту іншій особі;
- несанкціонований експорт;
- витік через вразливість;
- зараження шкідливим програмним забезпеченням;
- втрата або викрадення пристрою;
- помилка налаштування доступу;
- незаконні дії працівника чи підрядника;
- порушення з боку постачальника;
- знищення або пошкодження даних;

- тривала недоступність критичної інформації;
- інші події, що впливають на захист персональних даних.

18.3. Повідомлення про підозрюване порушення

Користувач, працівник, підрядник або інша особа, яка виявила або обґрунтовано підозрює порушення, повинна без необґрунтованої затримки повідомити Perevir через контактний канал, зазначений у цій Політиці.

18.4.Повідомлення бажано має містити:

- опис події;
- дату й приблизний час;
- спосіб виявлення;
- обліковий запис або функцію, яких стосується подія;
- категорії можливих даних;
- відомі наслідки;
- здійснені дії;
- контактні дані заявника;
- технічні матеріали, якщо вони наявні.

18.5.Особа, яка повідомляє про порушення, не повинна:

- самостійно отримувати несанкціонований доступ;
- копіювати надмірний обсяг даних;
- публічно розкривати вразливість до її усунення;
- вимагати винагороду під загрозою оприлюднення;
- перешкоджати роботі Системи;
- знищувати докази події.

18.6. Реєстрація та первинна оцінка

Після отримання інформації Perevir може:

- зареєструвати подію;
- визначити відповідальну команду;
- провести первинну технічну перевірку;
- установити, чи стосується подія персональних даних;
- визначити масштаб;
- класифікувати критичність;
- оцінити необхідність невідкладного обмеження доступу;
- залучити постачальника або корпоративного Користувача.

18.7. Локалізація порушення

Для припинення або обмеження порушення Perevir може:

- заблокувати обліковий запис;
- завершити активні сесії;
- відкликати токени й API-ключі;
- змінити права доступу;
- ізолювати компонент;
- тимчасово зупинити окрему функцію;
- заблокувати підозрілу IP-адресу;
- застосувати додаткові правила фільтрації;
- відключити інтеграцію;
- вимагати зміну пароля;
- залучити постачальника до припинення інциденту.

18.8.Заходи локалізації повинні бути пропорційними загрозі та, наскільки можливо, не створювати необґрунтованих обмежень для інших Користувачів.

18.9. Розслідування

Під час розслідування Perevir може визначати:

- причину порушення;
- дату початку та завершення;
- системи й компоненти, яких воно стосувалося;
- категорії персональних даних;
- приблизну кількість суб’єктів;
- приблизну кількість записів;
- осіб, які могли отримати доступ;
- можливість копіювання, зміни або знищення;
- наявні докази;
- фактичні та потенційні наслідки;
- заходи, необхідні для запобігання повторенню.

18.10.Під час розслідування Perevir може зберігати:

- журнали;
- копії конфігурацій;
- технічні образи;
- службове листування;
- записи дій;
- інші докази,

у мінімально необхідному обсязі та протягом строку, потрібного для розслідування і захисту прав.

18.11. Оцінювання ризику

Perevir оцінює ризик порушення для прав і свобод фізичних осіб з урахуванням:

- характеру даних;
- чутливості інформації;
- можливості ідентифікації;
- обсягу даних;
- кількості суб'єктів;
- характеру порушення;
- можливості незаконного використання;
- тривалості доступу;
- наявності шифрування;
- можливості відновлення;
- категорій постраждалих осіб;
- імовірності матеріальної або нематеріальної шкоди.

18.12.Можливі негативні наслідки можуть включати:

- викрадення особистості;
- шахрайство;
- фінансові втрати;
- втрату конфіденційності;
- дискримінацію;
- репутаційну шкоду;
- незаконне використання реєстрових даних;
- компрометацію облікового запису;
- переслідування;
- інші істотні обмеження прав фізичної особи.

18.13. Документування

Perevir документує порушення безпеки персональних даних у межах, необхідних для:

- встановлення обставин;
- оцінювання ризику;
- підтвердження прийнятих рішень;
- виконання договірних і законодавчих вимог;
- контролю виконання коригувальних заходів;
- удосконалення системи управління безпекою.

18.14.Запис про порушення може містити:

- дату виявлення;
- опис події;
- категорії даних;
- кількість суб'єктів;

- причину;
- наслідки;
- оцінку ризику;
- здійснені заходи;
- рішення щодо повідомлень;
- відповідальних осіб;
- стан виконання коригувальних дій.

18.15. Повідомлення корпоративного Користувача

Якщо Perevir виступає обробником або розпорядником, він повідомляє відповідного корпоративного Користувача про підтверджене порушення безпеки даних, які обробляються від його імені:

- без необґрунтованої затримки;
- у строк, установлений договором або Data Processing Agreement;
- із наданням доступної інформації, необхідної корпоративному Користувачу для виконання його обов’язків.

18.16.Повідомлення корпоративному Користувачу може містити:

- характер порушення;
- дату або орієнтовний період;
- категорії даних;
- приблизну кількість суб’єктів;
- відомі або ймовірні наслідки;
- здійснені заходи;
- рекомендовані дії;
- контакт для взаємодії.

18.17.Якщо всю інформацію неможливо надати одночасно, вона може передаватися поетапно без невиправданої затримки.

18.18. Повідомлення компетентного органу

Perevir повідомляє компетентний наглядовий або інший уповноважений орган про порушення, якщо такий обов’язок виникає відповідно до застосовного законодавства.

18.19.В Україні загальний порядок повідомлення Уповноваженого Верховної Ради України з прав людини стосується, зокрема, обробки, яка становить особливий ризик для прав і свобод суб’єктів. Тому необхідність і порядок повідомлення в конкретному випадку визначаються з урахуванням характеру обробки та чинних вимог Уповноваженого. (Законодавство України)

18.20.Якщо до обробки застосовується GDPR і порушення може створити ризик для прав і свобод фізичних осіб, відповідний контролер повідомляє компетентний наглядовий орган без невиправданої затримки та, за можливості, не пізніше ніж через 72 години після того, як йому стало відомо про порушення.

Якщо повідомлення подано пізніше, до нього додається пояснення причин затримки. (EUR-Lex)

18.21.Строк у 72 години застосовується лише тоді, коли конкретна обробка підпадає під дію GDPR. Він не повинен автоматично подаватися як універсальний строк для всіх операцій Perevir за законодавством України.

18.22. Повідомлення суб'єктів персональних даних

Perevir або відповідний корпоративний Користувач повідомляє постраждалих суб'єктів, якщо:

- цього вимагає застосовне законодавство;
- порушення може створити високий ризик для їхніх прав і свобод;
- повідомлення необхідне для зменшення можливої шкоди;
- таке повідомлення вимагає компетентний орган.

18.23.Повідомлення суб'єкту викладається зрозумілою мовою та може містити:

- опис характеру порушення;
- категорії даних;
- можливі наслідки;
- уже вжиті заходи;
- рекомендовані дії;
- контактні дані для звернення;
- іншу інформацію, передбачену законом.

18.24.Суб'єкту можуть рекомендувати:

- змінити пароль;
- завершити активні сесії;
- перевірити безпеку електронної пошти;
- відкликати API-ключ;
- бути уважним до фішингових повідомлень;
- перевірити операції у власних системах;
- звернутися до Perevir або відповідного корпоративного Користувача.

18.25.Індивідуальне повідомлення може не здійснюватися, якщо:

- ризик для суб'єктів відсутній або не є високим;

- дані були належним чином зашифровані й залишаються непридатними для стороннього використання;
- після порушення вжито заходів, які усунули високий ризик;
- повідомлення потребувало б непропорційних зусиль і закон дозволяє застосувати публічне або інше рівнозначне повідомлення;
- існує інша законна підстава не здійснювати повідомлення.

18.26. Взаємодія з постачальниками

Якщо порушення пов’язане з постачальником, Perevir може:

- вимагати невідкладної інформації;
- вимагати локалізації інциденту;
- отримувати журнали й технічні матеріали;
- брати участь у розслідуванні;
- вимагати коригувальний план;
- тимчасово призупинити передавання даних;
- припинити використання відповідного сервісу;
- реалізувати договірні засоби захисту.

18.27. Відновлення

Після локалізації порушення Perevir може:

- відновити дані з резервної копії;
- перевірити їх цілісність;
- замінити скомпрометовані ключі;
- змінити конфігурації;
- оновити програмне забезпечення;
- посилити контроль доступу;
- відновити функції поетапно;
- здійснювати посилений моніторинг.

18.28. Коригувальні та запобіжні заходи

За результатами розслідування Perevir може:

- усунути вразливість;
- змінити технічну архітектуру;
- переглянути права доступу;
- оновити процедури;
- провести навчання;
- змінити постачальника;
- переглянути строки зберігання;
- розширити журналювання;

- провести додаткове тестування;
- застосувати дисциплінарні або договірні заходи;
- актуалізувати оцінку ризику.

18.29. Perevir проводить аналіз причин порушення та, наскільки це доцільно, перевіряє ефективність упроваджених коригувальних заходів.

18.30. Конфіденційність розслідування

Інформація про порушення може бути обмежена в доступі, якщо її передчасне або надмірне розкриття:

- створює додаткову загрозу;
- перешкоджає розслідуванню;
- розкриває конфіденційні механізми захисту;
- порушує права інших осіб;
- суперечить законній вимозі компетентного органу.

18.31.Обмеження публічного розкриття не звільняє Perevir від обов'язкових повідомлень, передбачених застосовним законодавством або договором.

19. Права суб'єктів персональних даних

19.1.Суб'єкт персональних даних має права, передбачені законодавством України, а якщо до відповідної обробки застосовується GDPR - також права, установлені GDPR.

Права на персональні дані є невід'ємними та непорушними. Закон України «Про захист персональних даних» закріплює, зокрема, право знати про джерела збирання, місцезнаходження даних, мету обробки, отримувати доступ, заперечувати проти обробки, вимагати зміни або знищення даних та звертатися зі скаргами. (Законодавство України)

19.2.Обсяг конкретного права та порядок його реалізації залежать від:

- законодавства, що застосовується;
- ролі Perevir;
- категорії даних;
- джерела інформації;
- правової підстави;
- наявності законодавчих обмежень;
- прав і законних інтересів інших осіб.

19.3. Право знати про обробку

Суб’єкт має право знати:

- хто є володільцем або контролером даних;
- місцезнаходження володільця;
- склад і зміст персональних даних;
- мету обробки;
- правову підставу;
- джерела отримання;
- категорії одержувачів;
- строки або критерії зберігання;
- порядок реалізації своїх прав;
- інші відомості, передбачені законом.

19.4.Відповідна інформація може надаватися через:

- цю Політику;
- повідомлення під час реєстрації;
- налаштування облікового запису;
- договір;
- повідомлення про окрему функцію;
- відповідь на індивідуальний запит.

19.5. Право на доступ

Суб’єкт має право отримати підтвердження того, чи обробляє Perevir його персональні дані.

19.6.Якщо дані обробляються, суб’єкт може мати право отримати:

- доступ до даних;
- інформацію про мету;
- категорії персональних даних;
- категорії одержувачів;
- строки зберігання;
- джерело отримання;
- інформацію про права;
- інформацію про автоматизовану обробку, якщо вона здійснюється;
- копію персональних даних у передбачених законом випадках.

19.7.Право на доступ не повинно порушувати:

- права і свободи інших осіб;
- комерційну таємницю;
- права інтелектуальної власності;
- конфіденційність заходів інформаційної безпеки;

- законодавчо встановлені обмеження доступу;
- таємницю слідства або іншу захищену законом інформацію.

19.8. Право знати джерела отримання даних

Суб'єкт може звернутися за інформацією про джерело, з якого Perevir отримав його персональні дані, якщо розкриття такого джерела:

- не заборонене законом;
- не порушує права інших осіб;
- не створює загрози безпеці;
- є технічно та юридично можливим.

19.9.Якщо дані отримані з державного реєстру або офіційного ресурсу, Perevir може повідомити:

- найменування відповідного джерела;
- дату отримання або оновлення;
- характер отриманих відомостей;
- спосіб звернення до первинного держателя для виправлення даних.

19.10. Право на виправлення

Суб'єкт має право вимагати виправлення неточних, неповних або застарілих персональних даних.

19.11.Для виправлення Perevir може запросити:

- уточнення;
- документальне підтвердження;
- підтвердження особи;
- відомості про правильне значення;
- інформацію про джерело помилки.

19.12.Якщо неточні дані походять із зовнішнього реєстру, Perevir може:

- виправити лише власний запис або технічне відображення;
- оновити дані після виправлення первинного джерела;
- позначити інформацію як оскаржувану;
- надати суб'єкту інформацію про відповідного держателя;
- обмежити використання спірного запису в межах технічної можливості.

19.13. Perevir не має права самовільно змінювати офіційні відомості у державному реєстрі, держателем або адміністратором якого він не є.

19.14. Право на доповнення даних

Якщо дані є неповними, суб’єкт може надати додаткову інформацію або пояснення, якщо таке доповнення:

- відповідає меті обробки;
- є достовірним;
- не порушує прав інших осіб;
- може бути законно включене до відповідного набору даних.

19.15. Право вимагати видалення або знищення

Суб’єкт може вимагати видалення або знищення персональних даних, зокрема, якщо:

- дані більше не потрібні для первинної мети;
- правова підстава припинилася;
- згода відкликана і немає іншої підстави;
- обробка є незаконною;
- дані повинні бути видалені відповідно до закону;
- заперечення проти обробки має перевагу над законним інтересом Perevir.

Український закон передбачає видалення або знищення персональних даних, зокрема, після закінчення строку зберігання або припинення законної підстави обробки. (Законодавство України)

19.16.Право на видалення не є абсолютним. Дані можуть продовжувати зберігатися, якщо це необхідно для:

- виконання юридичного обов’язку;
- збереження бухгалтерської або податкової документації;
- здійснення права на інформацію;
- виконання завдання в суспільному інтересі;
- захисту інформаційної безпеки;
- встановлення, реалізації або захисту правових вимог;
- розслідування порушення;
- іншої передбаченої законом мети.

19.17.Видалення даних із Perevir не означає їх автоматичного видалення з:

- державного реєстру;
- судового рішення;
- офіційного вебресурсу;
- системи корпоративного Користувача;
- системи стороннього контролера;
- іншого незалежного джерела.

19.18. Право на обмеження обробки

Якщо застосовне законодавство передбачає таке право, суб’єкт може вимагати обмеження обробки, зокрема, коли:

- точність даних оскаржується;
- обробка є незаконною, але суб’єкт заперечує проти видалення;
- Perevir більше не потребує даних, але вони потрібні суб’єкту для правових вимог;
- суб’єкт заперечив проти обробки й триває оцінювання переважаючих підстав.

19.19.Під час обмеження дані можуть зберігатися, але інші операції з ними припиняються, крім випадків:

- наявності згоди;
- захисту правових вимог;
- захисту прав іншої особи;
- важливого суспільного інтересу;
- іншої підстави, передбаченої законом.

19.20. Право заперечувати проти обробки

Суб’єкт може подати вмотивоване заперечення проти обробки своїх персональних даних.

19.21. Perevir розглядає таке заперечення з урахуванням:

- правової підстави;
- мети обробки;
- законних інтересів Perevir або третьої особи;
- ризиків для суб’єкта;
- необхідності виконання договору або закону;
- необхідності захисту правових вимог.

19.22.Якщо законні підстави Perevir не переважають права суб’єкта, відповідна обробка припиняється або обмежується.

19.23. Право відмовитися від прямого маркетингу

Суб’єкт має право в будь-який момент відмовитися від використання його контактних даних для прямого маркетингу.

19.24.Після отримання заперечення Perevir припиняє відповідні маркетингові повідомлення, але може продовжувати надсилати:

- повідомлення про безпеку;
- інформацію про обліковий запис;
- повідомлення про технічні роботи;

- договірні повідомлення;
- іншу необхідну сервісну комунікацію.

19.25. Право відкликати згоду

Якщо обробка ґрунтується на згоді, суб’єкт може відкликати її в будь-який момент.

19.26.Відкликання згоди:

- не впливає на законність попередньої обробки;
- не припиняє обробку, для якої існує інша правова підстава;
- може призвести до припинення необов’язкової функції;
- не вимагає видалення документів, які повинні зберігатися за законом.

19.27. Право на перенесення даних

Якщо застосовується GDPR та виконані встановлені ним умови, суб’єкт може отримати надані ним персональні дані у структурованому, загальновживаному та машиночитаному форматі й передати їх іншому контролеру.

19.28.Право на перенесення зазвичай застосовується, коли:

- обробка ґрунтується на згоді або договорі;
- обробка здійснюється автоматизовано;
- передавання технічно можливе;
- реалізація права не порушує права інших осіб.

19.29.Право на перенесення не означає автоматичного права на отримання:

- усієї інформації з державних реєстрів;
- внутрішніх аналітичних моделей;
- комерційної таємниці;
- даних третіх осіб;
- технічних журналів безпеки в повному обсязі;
- об’єктів інтелектуальної власності Perevir.

19.30. Права щодо автоматизованих рішень

Якщо Perevir здійснює виключно автоматизоване прийняття рішень, яке має юридичні або аналогічно істотні наслідки для фізичної особи, суб’єкт може мати право:

- отримати інформацію про факт такої обробки;
- отримати загальне пояснення логіки;
- висловити свою позицію;
- вимагати участі людини;
- оскаржити рішення,

якщо такі права передбачені застосовним законодавством.

19.31.Індикатори ризику, технічні збіги та автоматично сформовані висновки Perevir:

- мають інформаційно-аналітичний характер;
- не встановлюють юридичного факту;
- не повинні бути єдиною підставою для рішення з істотними наслідками;
- мають перевірятися Користувачем з урахуванням первинних джерел та конкретних обставин.

19.32. Право на захист від незаконної обробки

Суб’єкт має право на захист своїх персональних даних від:

- незаконної обробки;
- випадкової втрати;
- знищення;
- пошкодження;
- неправомірного доступу;
- недостовірної інформації;
- інформації, що принижує честь, гідність або ділову репутацію, у випадках, передбачених законом.

19.33. Право на інформацію про порушення безпеки

Суб’єкт може бути повідомлений про порушення безпеки його персональних даних, якщо:

- такого повідомлення вимагає закон;
- порушення створює високий ризик для його прав і свобод;
- повідомлення необхідне для вжиття захисних заходів;
- компетентний орган вимагає здійснити повідомлення.

19.34. Право звернутися зі скаргою

Суб’єкт має право звернутися зі скаргою:

- до Perevir;
- до корпоративного Користувача, якщо він є володільцем або контролером;
- до Уповноваженого Верховної Ради України з прав людини;
- до іншого компетентного наглядового органу, якщо застосовується інше законодавство;
- до суду.

19.35.Звернення до Perevir не позбавляє суб’єкта права одночасно або надалі звернутися до компетентного органу чи суду.

19.36. Право на судовий захист

Суб’єкт має право захищати свої права в суді та вимагати передбачених законом способів захисту, зокрема:

- припинення незаконної обробки;
- виправлення або видалення даних;
- відшкодування шкоди;
- визнання дій незаконними;
- застосування іншого належного способу захисту.

19.37. Представництво

Суб’єкт може реалізовувати свої права:

- особисто;
- через законного представника;
- через представника за довіреністю;
- іншим передбаченим законом способом.

19.38. Perevir може запросити документ, що підтверджує повноваження представника.

19.39. Права щодо даних дітей і недієздатних осіб

Права дитини, недієздатної або обмежено дієздатної особи реалізуються:

- нею самостійно у випадках, передбачених законом;
- батьками;
- усиновлювачами;
- опікуном;
- піклувальником;
- іншим законним представником.

19.40. Обмеження прав

Окремі права можуть бути обмежені законом, якщо це необхідно і пропорційно для:

- національної безпеки;
- оборони;
- громадської безпеки;
- запобігання, розслідування або переслідування правопорушень;
- захисту прав інших осіб;
- виконання судового рішення;
- захисту професійної таємниці;
- інших передбачених законом цілей.

19.41. Perevir не обмежує права суб’єкта на власний розсуд. Будь-яке обмеження повинно мати належну правову підставу.

19.42. Визначення відповідальної сторони

Якщо запит стосується даних, щодо яких Perevir є самостійним володільцем або контролером, Perevir розглядає запит самостійно.

19.43.Якщо Perevir обробляє дані від імені корпоративного Користувача, він може:

- передати запит відповідному корпоративному Користувачу;
- повідомити суб’єкта про належного володільця або контролера;
- допомогти корпоративному Користувачу виконати запит;
- діяти відповідно до його документованої вказівки.

19.44.Якщо запит стосується первинних даних державного реєстру, суб’єкту може бути рекомендовано звернутися до:

- держателя реєстру;
- адміністратора;
- відповідного державного органу;
- особи, яка внесла відомості;
- іншого уповноваженого суб’єкта.

19.45.Перенаправлення до іншого володільця не звільняє Perevir від обов’язку розглянути ту частину запиту, яка стосується власної обробки, зокрема:

- відображення даних;
- кешування;
- історії запитів;
- сформованих звітів;
- похідної аналітики;
- технічних журналів;
- доступу до облікового запису.

19.46.Порядок подання запитів, підтвердження особи, строки відповіді та можливі підстави для відмови визначаються наступним розділом цієї Політики - **«Порядок реалізації прав суб’єктів персональних даних»**.

20. Порядок реалізації прав суб’єктів персональних даних

20.1.Для реалізації прав, передбачених цією Політикою та застосовним законодавством, суб’єкт персональних даних може звернутися до Perevir:

- електронною поштою;
- через форму зворотного зв’язку;
- через особистий кабінет, якщо відповідна функція доступна;
- письмово за місцезнаходженням Адміністрації;
- іншим способом, зазначеним у розділі «Контактна інформація».

20.2.Звернення може стосуватися, зокрема:

- отримання інформації про обробку;
- доступу до персональних даних;
- отримання копії даних;
- уточнення джерела їх отримання;
- виправлення або доповнення;
- видалення або знищення;
- обмеження обробки;
- заперечення проти обробки;
- відкликання згоди;
- відмови від маркетингових повідомлень;
- перенесення даних, якщо таке право застосовується;
- перегляду автоматизованого рішення;
- подання скарги щодо обробки;
- отримання інформації про порушення безпеки.

20.3. Зміст звернення

Для належного розгляду звернення суб’єкту рекомендується зазначити:

- прізвище, власне ім’я та по батькові, якщо воно використовується;
- контактну електронну адресу;
- інші контактні дані за необхідності;
- опис запитуваної дії;
- категорії персональних даних, яких стосується звернення;
- відомості про обліковий запис або організацію;
- обставини, за яких дані могли бути отримані Perevir;
- бажаний спосіб отримання відповіді;
- документи або пояснення, необхідні для розгляду вимоги.

20.4.У зверненні не потрібно зазначати пароль, особистий ключ КЕП, PIN-код Дія.Підпису, повні реквізити платіжної картки або інші секретні дані.

20.5. Перевірка особи заявника

До виконання звернення Perevir має право перевірити особу заявника, щоб запобігти:

- розкриттю персональних даних сторонній особі;

- незаконній зміні або видаленню інформації;
- захопленню облікового запису;
- шахрайству;
- зловживанню правами суб’єкта.

20.6.Для перевірки особи Perevir може використовувати:

- підтвердження через зареєстровану електронну адресу;
- вхід до облікового запису;
- контрольне підтвердження окремих даних;
- КЕП;
- Дія.Підпис;
- документ, що посвідчує особу, у мінімально необхідному обсязі;
- підтвердження повноважень представника;
- інший пропорційний спосіб.

20.7.Спосіб перевірки повинен відповідати:

- характеру запиту;
- категоріям даних;
- ризику незаконного розкриття;
- способу взаємодії із суб’єктом;
- доступним засобам ідентифікації.

20.8. Perevir не повинен вимагати надмірний обсяг документів, якщо особу можна надійно підтвердити менш втручальним способом.

20.9.Якщо Perevir не може надійно встановити особу заявника, він може:

- запросити додаткові відомості;
- тимчасово зупинити розгляд;
- відмовити у виконанні конкретної дії, яка створює ризик для прав іншої особи.

20.10. Звернення представника

Звернення може подаватися представником суб’єкта.

У такому разі Perevir може запросити:

- документ, що підтверджує особу представника;
- довіреність;
- документ про законне представництво;
- підтвердження обсягу повноважень;
- інші документи, передбачені законом.

20.11.Надання представнику доступу до персональних даних здійснюється лише в межах підтверджених повноважень.

20.12. Звернення щодо дитини або особи з обмеженою дієздатністю

Права дитини, недієздатної або обмежено дієздатної особи можуть реалізовуватися нею самостійно у випадках, передбачених законом, або через:

- батьків;
- усиновлювачів;
- опікуна;
- піклувальника;
- іншого законного представника.

20.13. Perevir може перевірити:

- статус законного представника;
- вік суб’єкта;
- межі представництва;
- відсутність конфлікту інтересів.

20.14. Реєстрація звернення

Отримане звернення може бути:

- зареєстроване;
- класифіковане за типом права;
- передане відповідальній особі;
- пов’язане з відповідним обліковим записом;
- зафіксоване в журналі звернень;
- збережене разом із відповіддю та матеріалами перевірки.

20.15.Дані звернення обробляються для:

- виконання вимоги суб’єкта;
- підтвердження законності дій Perevir;
- захисту прав сторін;
- виконання обов’язків перед наглядовими органами;
- удосконалення процесу розгляду звернень.

20.16. Первинний розгляд

Під час первинного розгляду Perevir визначає:

- чи є заявник суб’єктом відповідних даних;
- які дані та операції охоплює звернення;

- у якій ролі діє Perevir;
- чи є інший володілець або контролер;
- чи достатньо інформації для виконання;
- чи застосовуються законодавчі обмеження;
- чи може виконання порушити права інших осіб.

20.17. Строки розгляду за законодавством України

Якщо до звернення застосовується законодавство України, строк вивчення запиту щодо доступу до персональних даних не повинен перевищувати десяти робочих днів із дня його надходження.

Протягом цього строку заявнику повідомляється, чи буде запит задоволений, або зазначаються законні підстави для ненадання даних.

Запит задовольняється протягом тридцяти календарних днів із дня його надходження, якщо інший строк не встановлено законом. (Законодавство України)

20.18.Якщо звернення стосується не лише доступу, а й виправлення, видалення, заперечення або іншої дії, Perevir розглядає його у строки, визначені відповідною нормою законодавства, а за відсутності спеціального строку — без необґрунтованої затримки.

20.19. Строки за GDPR

Якщо до відповідної обробки застосовується GDPR, інформація про дії за запитом надається без невиправданої затримки та, як правило, протягом одного місяця з дня його отримання.

З урахуванням складності та кількості звернень цей строк може бути продовжений ще на два місяці з повідомленням суб’єкта про причини продовження. (EUR-Lex)

20.20.Якщо для підтвердження особи або уточнення звернення необхідна додаткова інформація, строк розгляду може обчислюватися з урахуванням дати її отримання відповідно до застосовного законодавства.

20.21. Уточнення звернення

Perevir може попросити суб’єкта уточнити звернення, якщо воно:

- сформульоване надто загально;
- стосується великого обсягу інформації;
- не дозволяє визначити конкретний обліковий запис;
- охоплює дані декількох осіб;
- містить суперечливі вимоги;
- не дозволяє визначити бажаний результат.

20.22.Уточнення не повинно використовуватися для необґрунтованого затягування розгляду або перешкоджання реалізації прав.

20.23. Формат відповіді

Відповідь може надаватися:

- електронною поштою;
- через особистий кабінет;
- у структурованому електронному файлі;
- у письмовій формі;
- іншим погодженим способом.

20.24.Якщо звернення надійшло в електронній формі, відповідь зазвичай надається в електронній формі, якщо заявник не попросив про інший спосіб і він є обґрунтованим.

20.25.Інформація надається:

- зрозумілою мовою;
- у доступній формі;
- без надмірних технічних подробиць;
- із поясненням істотних обмежень;
- із зазначенням можливості оскарження.

20.26. Копія персональних даних

У межах права на доступ Perevir може надати копію персональних даних, що стосуються заявника.

20.27.До копії можуть не включатися або можуть бути приховані:

- персональні дані інших осіб;
- паролі та автентифікаційні секрети;
- внутрішні механізми безпеки;
- інформація, доступ до якої обмежений законом;
- комерційна таємниця;
- захищені об’єкти інтелектуальної власності;
- службова інформація, розкриття якої створює загрозу.

20.28.Замість повної копії документа Perevir може надати:

- витяг;
- структурований набір даних;
- копію з прихованими відомостями третіх осіб;
- опис обробки;
- інший формат, який дозволяє реалізувати право без порушення прав інших осіб.

20.29. Виправлення даних

Якщо вимога про виправлення є обґрунтованою, Perevir:

- виправляє власні записи;
- доповнює неповні дані;
- оновлює відомості в обліковому записі;
- за потреби повідомляє одержувачів;
- фіксує факт і дату виправлення.

20.30.Якщо інформація походить із державного або незалежного зовнішнього джерела, Perevir може:

- оновити власну копію після зміни першоджерела;
- позначити дані як спірні;
- обмежити їх відображення, якщо це законно і технічно можливо;
- запропонувати звернутися до держателя або адміністратора джерела.

20.31. Perevir не може самостійно змінювати запис у реєстрі, держателем або адміністратором якого він не є.

20.32. Видалення даних

Перед видаленням Perevir перевіряє:

- чи досягнута мета обробки;
- чи припинилася правова підстава;
- чи існує юридичний обов’язок зберігання;
- чи необхідні дані для спору;
- чи стосуються вони інших осіб;
- чи є Perevir самостійним контролером або обробником;
- чи може бути застосоване обмеження замість видалення.

20.33.Якщо вимога задовольняється, дані можуть бути:

- видалені з активних систем;
- знеособлені;
- заблоковані;
- виключені з подальшого використання;
- видалені після завершення технічного циклу резервного копіювання.

20.34.Запис про виконання вимоги або мінімальна інформація, необхідна для підтвердження видалення, може зберігатися на окремій правовій підставі.

20.35. Обмеження обробки

У разі обмеження Perevir може:

- позначити відповідні дані;
- призупинити їх використання;
- заборонити зміну;
- відключити від окремих функцій;
- обмежити доступ;
- продовжити зберігання лише для законно дозволених цілей.

20.36. Заперечення проти обробки

Під час розгляду заперечення Perevir оцінює:

- підставу обробки;
- обставини суб’єкта;
- характер законного інтересу;
- необхідність подальшої обробки;
- ризики для прав суб’єкта;
- можливість припинення або мінімізації операцій.

20.37.Якщо заперечення стосується прямого маркетингу, відповідна маркетингова обробка припиняється без необхідності додаткового балансування інтересів.

20.38. Відкликання згоди

Згода може бути відкликана:

- через налаштування облікового запису;
- через посилання для відписки;
- шляхом звернення до Perevir;
- іншим доступним способом.

20.39.Відкликання згоди не припиняє обробку, яка:

- здійснюється на іншій правовій підставі;
- необхідна для виконання закону;
- потрібна для захисту правових вимог;
- стосується обов’язкових сервісних повідомлень;
- була законно здійснена до відкликання.

20.40. Перенесення даних

Якщо право на перенесення застосовується, Perevir може надати дані:

- у форматі CSV;
- JSON;

- XML;
- іншому структурованому та машиночитаному форматі.

20.41.Пряме передавання іншому контролеру здійснюється лише тоді, коли:

- воно технічно можливе;
- одержувача можна надійно ідентифікувати;
- передавання не порушує права інших осіб;
- існує належний захищений канал.

20.42. Безоплатність

Розгляд і виконання обґрунтованого звернення зазвичай здійснюються безоплатно.

20.43.Якщо запит є явно необґрунтованим або надмірним, зокрема через систематичне повторення, Perevir може в межах, дозволених законом:

- вимагати обґрунтовану плату за адміністративні витрати;
- відмовити у виконанні запиту;
- обмежити відповідь інформацією, необхідною для реалізації права.

20.44.Обов’язок довести необґрунтованість або надмірність звернення покладається на сторону, яка посилається на цю обставину.

20.45. Підстави для повної або часткової відмови

Perevir може відмовити в задоволенні звернення повністю або частково, якщо:

- особу заявника не підтверджено;
- заявник не має належних повноважень;
- дані не обробляються Perevir;
- виконання прямо заборонене законом;
- дані необхідні для юридичного обов’язку;
- інформація потрібна для захисту правових вимог;
- запит порушує права інших осіб;
- доступ обмежений режимом відповідного реєстру;
- запит є явно необґрунтованим або надмірним;
- застосовується інша передбачена законом підстава.

20.46.Відмова повинна містити:

- причину;
- правову або фактичну підставу;
- інформацію про можливість уточнення;
- спосіб оскарження;
- контакт компетентного наглядового органу, якщо це застосовується.

20.47. Роль корпоративного Користувача

Якщо Perevir обробляє відповідні дані від імені корпоративного Користувача, Perevir може:

- передати звернення корпоративному Користувачу;
- повідомити заявника про належного контролера;
- виконати документовану вказівку корпоративного Користувача;
- надати технічну допомогу в пошуку, виправленні, експорті або видаленні даних.

20.48.Корпоративний Користувач несе відповідальність за прийняття рішення щодо звернення, якщо саме він визначає цілі та істотні засоби обробки.

20.49. Perevir самостійно розглядає частину звернення, яка стосується даних, щодо яких він виступає окремим володільцем або контролером, зокрема:

- реєстраційних даних;
- даних безпеки;
- журналів власної інфраструктури;
- договірних та платіжних відомостей;
- звернень до підтримки.

20.50. Повідомлення одержувачів

Якщо персональні дані були виправлені, видалені або обмежені, Perevir може повідомити про це одержувачів, яким вони раніше передавалися, якщо:

- це вимагається законом;
- повідомлення є технічно можливим;
- воно не потребує непропорційних зусиль;
- одержувач не має незалежної правової підстави для зберігання.

20.51. Оскарження

Суб’єкт може оскаржити рішення або бездіяльність Perevir:

- шляхом повторного звернення;
- шляхом подання скарги відповідальній особі Perevir;
- до Уповноваженого Верховної Ради України з прав людини;
- до компетентного наглядового органу іншої держави, якщо це застосовується;
- до суду.

Права на доступ, зміну або знищення даних, заперечення проти обробки та подання скарг прямо передбачені Законом України «Про захист персональних даних». (Законодавство України)

21. Автоматизований аналіз та індикатори ризику

21.1. Perevir може використовувати автоматизовані інформаційно-аналітичні засоби для:

- пошуку інформації;
- структурування даних;
- нормалізації записів;
- зіставлення відомостей із різних джерел;
- виявлення збігів;
- побудови зв’язків;
- формування часових ліній;
- виявлення змін;
- формування інформаційних індикаторів;
- ранжування результатів;
- виявлення аномалій;
- підготовки аналітичних звітів.

21.2.

Автоматизований аналіз може стосуватися:

- юридичних осіб;
- фізичних осіб - підприємців;
- керівників;
- засновників;
- учасників;
- бенефіціарних власників;
- представників;
- посадових осіб;
- інших фізичних осіб, відомості про яких законно містяться у відповідних джерелах.

21.3. Джерела автоматизованого аналізу

Для автоматизованого аналізу можуть використовуватися:

- державні реєстри;
- офіційні інформаційні системи;
- відкриті набори даних;
- судові та виконавчі відомості;
- дані про публічні закупівлі;
- санкційні переліки;
- ліцензовані комерційні джерела;

- інформація, надана Користувачем;
- результати попередніх законних перевірок;
- технічні метадані.

21.4.Використання певного джерела в аналітичному модулі не означає, що Perevir:

- є держателем або адміністратором такого джерела;
- гарантує його повноту;
- контролює дату оновлення;
- має право самостійно змінювати первинні записи.

21.5. Нормалізація та зіставлення

Perevir може автоматично:

- приводити назви й ідентифікатори до єдиного формату;
- усувати технічні дублікати;
- зіставляти записи за кодами та іншими ідентифікаторами;
- визначати ймовірні збіги;
- пов’язувати записи з різних джерел;
- визначати зміни в часі;
- формувати історичні послідовності.

21.6.Ймовірний збіг не завжди означає, що записи стосуються однієї й тієї самої особи.

Особливо це стосується збігів, сформованих лише за:

- ПІБ;
- частиною імені;
- адресою;
- місцем роботи;
- іншими неунікальними ознаками.

21.7.Користувач зобов’язаний перевіряти такі збіги за додатковими ідентифікаторами та первинними джерелами.

21.8. Індикатори ризику

Perevir може формувати умовні індикатори, які вказують на наявність певної події, ознаки або комбінації даних.

21.9.Індикатори можуть стосуватися, наприклад:

- припинення або зміни реєстраційного статусу;
- зміни керівника або власників;
- судових спорів;

- виконавчих проваджень;
- банкрутства;
- санкційних збігів;
- податкового статусу;
- анулювання ліцензії;
- істотних змін у публічних закупівлях;
- зв’язків між суб’єктами;
- суперечностей між джерелами;
- нетипової динаміки відомостей;
- інших визначених інформаційних факторів.

21.10.Конкретний склад індикаторів може залежати від:

- обраного модуля;
- тарифного плану;
- доступних джерел;
- налаштувань Користувача;
- галузі або сценарію перевірки;
- змін функціональності Perevir.

21.11. Інформаційний характер індикаторів

Індикатор ризику:

- не є юридичним висновком;
- не встановлює факту правопорушення;
- не підтверджує недоброчесність особи;
- не є кредитним рейтингом, якщо прямо не зазначено інше;
- не є гарантією наявності або відсутності ризику;
- не замінює професійну юридичну, фінансову чи комплаєнс-перевірку;
- не повинен бути єдиною підставою для рішення з істотними наслідками.

21.12.Відсутність індикатора не означає:

- відсутність будь-якого ризику;
- повноту інформації;
- відсутність події в іншому джерелі;
- актуальність усіх первинних даних;
- гарантію добросовісності суб’єкта.

21.13.Наявність індикатора не означає автоматично:

- вину;
- шахрайство;
- неплатоспроможність;

- незаконну діяльність;
- неприйнятність співпраці;
- необхідність відмови в послузі або працевлаштуванні.

21.14. Формування оцінок і рівнів

Якщо Perevir використовує числовий бал, категорію, позначку або рівень ризику, такий результат може формуватися на основі:

- кількості виявлених подій;
- типу події;
- актуальності даних;
- надійності джерела;
- повторюваності;
- взаємозв’язку декількох факторів;
- правил відповідного аналітичного модуля.

21.15.Методика оцінювання може змінюватися внаслідок:

- появи нових джерел;
- зміни структури даних;
- виправлення помилок;
- перегляду вагових коефіцієнтів;
- зміни законодавства;
- удосконалення аналітичних моделей.

21.16.Зміна методики може призвести до зміни результату без зміни первинних даних.

21.17. Пояснюваність результату

Наскільки це технічно й юридично можливо, Perevir може відображати:

- фактори, що вплинули на індикатор;
- джерело відповідної інформації;
- дату отримання або оновлення;
- категорію події;
- зв’язок між вхідними даними та результатом;
- застереження щодо обмежень.

21.18. Perevir не зобов’язаний розкривати:

- програмний код;
- комерційну таємницю;
- повну архітектуру алгоритму;
- заходи протидії шахрайству;
- технічні параметри, розкриття яких створює загрозу безпеці;

- права інтелектуальної власності третіх осіб.

21.19.Водночас обмеження розкриття не повинно позбавляти суб’єкта права отримати змістовну інформацію про логіку, значення та можливі наслідки автоматизованої обробки, коли таке право прямо передбачено застосовним законодавством.

21.20. Профілювання

Окремі функції Perevir можуть відповідати ознакам профілювання, якщо автоматизована обробка використовується для оцінювання або прогнозування певних аспектів, пов’язаних із фізичною особою.

21.21.Профілювання може стосуватися:

- професійної або підприємницької діяльності;
- корпоративних зв’язків;
- участі в юридичних особах;
- судової або виконавчої історії;
- санкційних чи регуляторних факторів;
- поведінки Користувача в Системі;
- безпекового ризику облікового запису.

21.22. Perevir не повинен використовувати профілювання для:

- незаконної дискримінації;
- прихованого маніпулювання;
- визначення чутливих характеристик без належної підстави;
- створення висновків, не пов’язаних із визначеною метою;
- необґрунтованого позбавлення людини прав або можливостей.

21.23. Автоматизовані рішення з істотними наслідками

За загальним правилом Perevir надає Користувачу інформаційно-аналітичний інструмент і не приймає від свого імені остаточні рішення щодо:

- укладення договору з перевіреною особою;
- прийняття на роботу;
- звільнення;
- надання кредиту;
- встановлення ціни;
- надання соціальної або іншої суттєвої послуги;
- включення до внутрішнього «чорного списку»;
- застосування дисциплінарного заходу;
- інших рішень із юридичними або аналогічно істотними наслідками.

21.24.Такі рішення, якщо вони приймаються, ухвалює Користувач або інша відповідальна особа.

21.25.Користувач повинен забезпечити:

- участь уповноваженої людини;
- оцінювання контексту;
- перевірку актуальності даних;
- перевірку первинних джерел;
- можливість особи надати пояснення;
- недискримінаційність;
- документування підстав істотного рішення.

21.26.Якщо окрема функція Perevir у майбутньому передбачатиме виключно автоматизоване рішення з юридичними або аналогічно істотними наслідками, до початку такої обробки повинні бути визначені:

- конкретна мета;
- правова підстава;
- логіка обробки;
- категорії даних;
- можливі наслідки;
- право на втручання людини;
- спосіб оскарження;
- додаткові заходи захисту.

GDPR передбачає право особи не підлягати рішенню, заснованому виключно на автоматизованій обробці, включно з профілюванням, якщо таке рішення створює юридичні або аналогічно істотні наслідки, за винятком установлених Регламентом випадків. (EUR-Lex)

21.27. Людський перегляд

Коли застосовне право на перегляд автоматизованого результату, суб’єкт може звернутися з вимогою:

- пояснити основні фактори;
- перевірити правильність вхідних даних;
- виправити неточності;
- залучити уповноважену людину;
- висловити власну позицію;
- оскаржити результат.

21.28.Людський перегляд не повинен бути формальним. Уповноважена особа повинна мати можливість:

- оцінити обставини;
- перевірити джерела;
- не погодитися з автоматизованим результатом;
- змінити або скасувати відповідне рішення;
- документувати підстави висновку.

21.29. Точність та якість

Perevir вживає розумних заходів для:

- перевірки технічної коректності алгоритмів;
- контролю якості зіставлення;
- виявлення систематичних помилок;
- оновлення джерел;
- тестування змін;
- позначення рівня впевненості;
- усунення виявлених дефектів.

21.30. Perevir не може гарантувати абсолютну точність автоматизованого аналізу через:

- помилки в первинних джерелах;
- затримку оновлення;
- однакові або схожі ідентифікатори;
- неповні записи;
- технічні обмеження інтеграцій;
- неоднозначність інформації;
- зміну правового чи фактичного статусу особи.

21.31. Недопущення упередженості

Під час розроблення аналітичних моделей Perevir може оцінювати ризик:

- необґрунтованої дискримінації;
- систематичних помилок;
- надмірного впливу окремого фактора;
- нерівномірної якості даних;
- помилкового ототожнення;
- непропорційного негативного результату.

21.32.Спеціальні категорії персональних даних не повинні використовуватися для автоматизованого оцінювання, крім випадків, коли:

- це прямо дозволено законом;
- існує спеціальна правова підстава;
- застосовані додаткові гарантії;

- обробка є необхідною та пропорційною.

21.33. Моніторинг моделей

Perevir може здійснювати:

- тестування точності;
- контроль помилкових збігів;
- аналіз скарг;
- перегляд правил оцінювання;
- перевірку якості джерел;
- аудит суттєвих змін;
- документування версій методики.

21.34.Результати автоматизованого аналізу можуть зберігатися разом із:

- датою формування;
- версією методики;
- використаними джерелами;
- параметрами запиту;
- поясненнями та застереженнями;
- подальшими виправленнями.

21.35. Відповідальність Користувача

Користувач, який використовує індикатори або аналітичні результати, зобов’язаний:

- використовувати їх лише для законної мети;
- перевіряти критично важливі дані;
- не подавати індикатор як доведений факт;
- не поширювати необґрунтовані негативні висновки;
- враховувати дату та джерело;
- не приймати непропорційне рішення;
- надати особі можливість пояснити суперечливі дані, коли це необхідно;
- дотримуватися вимог щодо захисту персональних даних.

22. Дані третіх осіб, які використовує Користувач

22.1.Під час використання Perevir Користувач може:

- вводити персональні дані третьої особи;
- виконувати пошук щодо фізичної особи;
- додавати особу до моніторингу;

- завантажувати файл із персональними даними;
- передавати дані через API;
- створювати внутрішні коментарі;
- формувати та зберігати звіти;
- передавати інформацію через інтеграцію;
- іншим способом використовувати дані осіб, які не є Користувачами Perevir.

22.2.До таких осіб можуть належати:

- працівники;
- кандидати;
- клієнти;
- контрагенти;
- представники контрагентів;
- фізичні особи - підприємці;
- засновники;
- керівники;
- бенефіціарні власники;
- позичальники;
- поручителі;
- постачальники;
- учасники судових або виконавчих проваджень;
- інші особи.

22.3. Відповідальність Користувача

Користувач самостійно відповідає за законність використання персональних даних третіх осіб, зокрема за:

- наявність визначеної мети;
- належну правову підставу;
- пропорційність перевірки;
- допустимість джерела;
- інформування суб’єкта, якщо воно є обов’язковим;
- дотримання строків зберігання;
- реалізацію прав суб’єкта;
- законність рішень, прийнятих за результатами перевірки.

22.4.Надання Perevir технічної можливості ввести, перевірити, зберегти або проаналізувати дані не означає підтвердження законності конкретної дії Користувача.

22.5. Правова підстава

До використання даних третьої особи Користувач повинен визначити належну правову підставу, зокрема:

- згоду;
- необхідність укладення або виконання договору;
- виконання юридичного обов’язку;
- законний інтерес;
- дозвіл, наданий законом;
- захист правових вимог;
- іншу передбачену законом підставу.

22.6.Згода не є обов’язковою в усіх випадках, однак Користувач не може використовувати відсутність вимоги щодо згоди як підставу для необмеженої або несумісної обробки.

22.7. Визначеність мети

Користувач повинен до початку обробки визначити конкретну мету, наприклад:

- перевірку потенційного контрагента;
- виконання комплаєнс-процедури;
- запобігання шахрайству;
- перевірку повноважень;
- виконання законодавчої вимоги;
- оцінювання ризику договірних відносин;
- захист прав у спорі.

22.8.Не допускається використання Perevir для невизначеної мети «про всяк випадок», якщо таке використання призводить до надмірного збирання, тривалого моніторингу або створення необґрунтованого профілю особи.

22.9. Мінімізація

Користувач повинен вводити або завантажувати лише ті дані, які:

- необхідні для визначеної мети;
- пов’язані з відповідною особою;
- є пропорційними;
- законно отримані;
- не є надмірними.

22.10.Зокрема, Користувач не повинен без необхідності завантажувати:

- копії паспортів;
- повні податкові номери;
- домашні адреси;
- дані банківських рахунків;
- медичну інформацію;

- біометричні дані;
- приватне листування;
- відомості про дітей;
- інші чутливі або надмірні дані.

22.11. Достовірність

Користувач повинен уживати розумних заходів для перевірки:

- правильності введених даних;
- належності даних конкретній особі;
- актуальності;
- відповідності джерела;
- відсутності явної помилки;
- правильності сформованих висновків.

22.12.Особливу увагу слід приділяти випадкам, коли особи мають:

- однакове ПІБ;
- схожі назви;
- однакові дати народження;
- спільну адресу;
- інші неунікальні ознаки.

22.13. Інформування третьої особи

Якщо закон вимагає інформування особи, Користувач повинен повідомити їй, зокрема:

- хто обробляє дані;
- для якої мети;
- на якій підставі;
- які категорії даних використовуються;
- з яких джерел їх отримано;
- кому вони можуть передаватися;
- як довго зберігатимуться;
- як реалізувати права.

22.14.Обов’язок інформування може не застосовуватися лише у випадках, прямо передбачених законодавством.

22.15. Спеціальні категорії даних

Користувачу заборонено завантажувати або цілеспрямовано обробляти через Perevir спеціальні категорії персональних даних, якщо:

- така функція прямо не передбачена;

- відсутня спеціальна правова підстава;
- не застосовані необхідні заходи захисту;
- обробка не погоджена з Perevir, коли це необхідно.

22.16.До спеціальних категорій належать, зокрема, дані про:

- расове чи етнічне походження;
- політичні переконання;
- релігійні або світоглядні переконання;
- членство у професійних спілках;
- генетичні дані;
- біометричні дані для унікальної ідентифікації;
- здоров’я;
- статеве життя;
- сексуальну орієнтацію.

22.17. Дані про правопорушення

Використання інформації про кримінальні правопорушення, судимості, адміністративні правопорушення або розслідування допускається лише:

- за наявності належної правової підстави;
- для конкретної та законної мети;
- в обсязі, дозволеному законом;
- із врахуванням презумпції невинуватості;
- без ототожнення процесуального статусу з доведеною виною.

22.18.Факт згадування особи в судовій справі, кримінальному провадженні або виконавчому документі сам по собі не підтверджує її неправомірної поведінки.

22.19. Дані дітей

Perevir не призначений для систематичного створення профілів дітей.

22.20.Користувач може обробляти дані дитини лише тоді, коли:

- це необхідно для законної мети;
- існує належна правова підстава;
- враховані найкращі інтереси дитини;
- застосовані підвищені заходи захисту;
- обробка не є надмірною.

22.21. Моніторинг третіх осіб

До додавання особи до постійного або регулярного моніторингу Користувач повинен оцінити:

- необхідність моніторингу;
- його тривалість;
- частоту перевірок;
- категорії подій;
- обґрунтовані очікування особи;
- можливий вплив на її права;
- можливість досягнення мети менш втручальним способом.

22.22.Регулярний моніторинг не повинен бути:

- безстроковим без перегляду необхідності;
- прихованим переслідуванням;
- засобом особистого контролю;
- способом тиску;
- інструментом незаконного стеження;
- несумісним із професійною або договірною метою.

22.23. Заборонене використання

Користувачу заборонено використовувати Perevir для:

- переслідування;
- шантажу;
- погроз;
- дискримінації;
- незаконного спостереження;
- доксингу;
- публічного приниження;
- поширення недостовірної інформації;
- створення незаконних «чорних списків»;
- викрадення особистості;
- шахрайства;
- незаконного стягнення боргу;
- спаму;
- несанкціонованого маркетингу;
- іншої протиправної мети.

22.24.Користувачу також заборонено:

- масово завантажувати дані без законної мети;
- обходити технічні обмеження;
- використовувати ботів або скрипти без дозволу;
- об’єднувати дані для створення надмірних профілів;
- намагатися визначити чутливі характеристики;
- передавати доступ невизначеному колу осіб;

- використовувати результати поза межами початкової мети.

22.25. Завантажені матеріали

Якщо Користувач завантажує до Perevir документи, таблиці, списки або інші матеріали, він підтверджує, що:

- має право на їх використання;
- має право передати їх Perevir;
- матеріали не містять незаконно отриманих даних;
- обсяг інформації є пропорційним;
- передавання не порушує зобов'язань конфіденційності;
- обробка відповідає заявленій меті.

22.26. Perevir не зобов'язаний здійснювати попередню юридичну перевірку кожного завантаженого файлу.

22.27.Водночас Perevir може:

- обмежити завантаження;
- заблокувати файл;
- призупинити обробку;
- попросити пояснити правову підставу;
- вимагати видалення надмірних даних;
- заблокувати обліковий запис;
- повідомити компетентний орган у випадках, передбачених законом.

22.28. Дані через API та інтеграції

Під час передавання даних третіх осіб через API або зовнішню інтеграцію Користувач відповідає за:

- законність джерела;
- налаштування обсягу передавання;
- автентифікацію системи;
- захист API-ключів;
- визначення одержувачів;
- строки зберігання;
- безпеку власної інформаційної системи.

22.29. Perevir може встановлювати:

- технічні ліміти;
- перелік дозволених полів;
- вимоги до шифрування;
- правила журналювання;

- заборону передавання окремих категорій даних;
- додаткові умови API.

22.30. Експорт і подальше використання

Після експорту звіту або даних Користувач стає відповідальним за:

- безпечне зберігання;
- обмеження доступу;
- подальше передавання;
- видалення;
- захист від витоку;
- дотримання первинної мети;
- реалізацію прав суб'єкта у власній системі.

22.31. Perevir не контролює всі подальші операції після законного експорту, але може застосовувати:

- журналювання;
- водяні знаки;
- обмеження масового експорту;
- персоналізовані ідентифікатори звітів;
- інші засоби підзвітності.

22.32. Рішення щодо третьої особи

Користувач не повинен приймати рішення з істотними наслідками для третьої особи виключно на підставі:

- одного реєстрового запису;
- автоматичного індикатора;
- ймовірного збігу;
- застарілої інформації;
- неперевіреного зовнішнього джерела;
- відсутності даних у Perevir.

22.33.До прийняття істотного рішення Користувачу рекомендується:

- перевірити первинне джерело;
- зіставити унікальні ідентифікатори;
- оцінити дату актуальності;
- перевірити контекст;
- отримати пояснення особи;
- залучити уповноваженого спеціаліста;
- документувати підстави рішення.

22.34. Звернення третьої особи

Якщо третя особа звертається до Perevir щодо даних, які ввів або використовує Користувач, Perevir може:

- визначити відповідний обліковий запис;
- повідомити Користувача;
- передати йому звернення;
- обмежити відповідну обробку;
- надати технічну допомогу;
- самостійно розглянути частину звернення, що стосується власної обробки.

22.35.Користувач зобов’язаний співпрацювати з Perevir під час розгляду:

- запиту суб’єкта;
- скарги;
- вимоги компетентного органу;
- інциденту безпеки;
- спору щодо законності даних;
- вимоги про виправлення або видалення.

22.36. Видалення даних третьої особи

Користувач повинен видалити або знеособити дані третьої особи, коли:

- мету досягнуто;
- договір припинено;
- правова підстава втрачена;
- строк зберігання закінчився;
- вимога суб’єкта є обґрунтованою;
- дані визнані незаконно отриманими;
- подальше використання стало надмірним.

22.37. Відповідальність за порушення

У разі порушення цього розділу Perevir може:

- попередити Користувача;
- вимагати припинення обробки;
- обмежити функцію;
- видалити незаконний матеріал;
- призупинити або заблокувати обліковий запис;
- припинити договір;
- зберегти докази порушення;
- звернутися до компетентного органу;
- застосувати інші передбачені договором або законом заходи.

22.38.Користувач несе відповідальність за власні незаконні дії з даними третіх осіб відповідно до:

- законодавства;
- договору;
- Правил користування;
- Data Processing Agreement;
- правил API;
- інших застосовних документів.

22.39. Perevir не звільняється від власної відповідальності за ті операції, в яких він самостійно визначає цілі та істотні засоби обробки або порушує власні обов’язки щодо захисту персональних даних.

23. Конфіденційність дітей

23.1. Perevir є професійною інформаційно-аналітичною системою, призначеною для використання юридичними особами, фізичними особами — підприємцями, державними органами, адвокатами, нотаріусами, аудиторами, комплаєнс-фахівцями та іншими повнолітніми користувачами, які здійснюють законну професійну діяльність.

23.2. Perevir не призначений для використання дітьми та не спрямований на залучення осіб, які не досягли повноліття, якщо інше прямо не передбачено законодавством.

23.3.Адміністрація Perevir не здійснює свідомого збору персональних даних дітей як окремої категорії користувачів.

23.4.Якщо Perevir стане відомо, що обліковий запис був створений дитиною без належної правової підстави або необхідної згоди законного представника у випадках, коли така згода є обов'язковою, Perevir може:

- призупинити використання облікового запису;
- вимагати підтвердження віку;
- вимагати підтвердження повноважень законного представника;
- обмежити окремі функції;
- видалити обліковий запис;
- видалити відповідні персональні дані;
- вжити інших заходів, необхідних для виконання законодавства.

23.5.Якщо Користувач використовує Perevir для законної обробки персональних даних дітей (наприклад, відповідно до вимог законодавства, судового рішення або під час виконання службових повноважень), саме Користувач відповідає за:

- визначення належної правової підстави;

- дотримання принципу мінімізації;
- забезпечення додаткових гарантій захисту;
- виконання вимог законодавства щодо дітей;
- реалізацію прав законних представників.

23.6. Perevir рекомендує уникати завантаження або обробки персональних даних дітей, якщо відповідної законної необхідності не існує.

23.7.У разі отримання обґрунтованого звернення законного представника щодо персональних даних дитини Perevir розглядає таке звернення відповідно до законодавства та розділу **«Порядок реалізації прав суб'єктів персональних даних»** цієї Політики.

24. Звернення державних органів

24.1. Perevir може отримувати запити, вимоги, ухвали, постанови або інші документи від державних органів, органів місцевого самоврядування, судів, правоохоронних органів та інших уповноважених суб'єктів.

24.2.До розкриття персональних даних Perevir перевіряє, наскільки це можливо:

- компетенцію органу;
- законність запиту;
- повноваження посадової особи;
- форму документа;
- правову підставу;
- обсяг запитуваної інформації;
- співмірність вимоги;
- наявність законодавчих обмежень.

24.3. Perevir передає лише той обсяг інформації, який:

- прямо вимагається законом;
- необхідний для виконання відповідної вимоги;
- є пропорційним меті запиту.

24.4.Якщо запит є неповним, суперечить законодавству або не дозволяє однозначно встановити його законність, Perevir може:

- вимагати уточнення;
- вимагати додаткові документи;
- обмежити обсяг інформації;
- відмовити у наданні інформації;
- оскаржити відповідну вимогу у випадках, передбачених законом.

24.5.Якщо закон прямо не забороняє повідомлення суб'єкта персональних даних, Perevir може повідомити його про отримання відповідного запиту.

24.6.Якщо Perevir виступає лише розпорядником (процесором) персональних даних корпоративного Користувача, Perevir, наскільки це дозволено законодавством, може:

- повідомити корпоративного Користувача про отриманий запит;
- передати запит відповідному володільцю або контролеру;
- діяти відповідно до документованих вказівок корпоративного Користувача;
- самостійно надати інформацію лише тоді, коли цього прямо вимагає закон.

24.7.Факт отримання запиту державного органу сам по собі не означає, що Perevir зобов'язаний автоматично розкрити всю запитувану інформацію.

24.8. Perevir документує випадки розкриття персональних даних державним органам у межах, необхідних для:

- підтвердження законності розкриття;
- захисту прав Користувачів;
- виконання законодавства;
- внутрішнього аудиту;
- розгляду можливих спорів.

25. Зміни до Політики

25.1. Perevir має право періодично змінювати, доповнювати або оновлювати цю Політику конфіденційності.

25.2.Зміни можуть здійснюватися, зокрема, у зв'язку з:

- змінами законодавства;
- змінами функціональності Perevir;
- впровадженням нових сервісів;
- зміною способів обробки персональних даних;
- зміною категорій персональних даних;
- зміною постачальників;
- зміною міжнародних механізмів передавання даних;
- результатами аудитів;
- появою нових ризиків інформаційної безпеки;
- рішеннями судів або компетентних органів.

25.3.Нова редакція Політики набирає чинності з моменту її опублікування на офіційному вебсайті Perevir, якщо інше прямо не зазначено у відповідній редакції.

25.4.У разі внесення істотних змін, які можуть вплинути на права Користувачів або порядок обробки персональних даних, Perevir може додатково повідомити Користувачів шляхом:

- повідомлення в особистому кабінеті;
- електронного листа;
- повідомлення в інтерфейсі Системи;
- публікації відповідного повідомлення на офіційному вебсайті;
- іншого доступного способу інформування.

25.5.Продовження використання Perevir після набрання чинності новою редакцією Політики означає, що Користувач ознайомився з відповідними змінами, якщо інше не передбачено законодавством.

25.6.Якщо окремі зміни потребують отримання нової згоди Користувача відповідно до застосовного законодавства, Perevir отримає таку згоду до початку відповідної обробки.

25.7.Попередні редакції Політики можуть зберігатися Perevir для:

- підтвердження історії змін;
- виконання юридичних обов'язків;
- вирішення спорів;
- внутрішнього аудиту;
- підтвердження умов, що діяли на певний момент часу.

26. Контактна інформація

26.1.Адміністратором інформаційної системи **Perevir** та особою, відповідальною за організацію надання доступу до Системи, є:

Товариство з обмеженою відповідальністю «БІНОТЕЛ АЙТІ-СЕРВІС»

26.2. Юридична адреса

02081, Україна,
м. Київ,
вул. Здолбунівська, 7Д, корпус 3,
Бізнес-центр «Аполло», 2 поверх.

26.3. Контактні дані з питань використання Perevir

Електронна пошта: support@perevir.ua

Телефони:

- +38 (044) 344-04-44
- +38 (067) 344-04-44 (багатоканальний)
- +38 (050) 344-04-44 (багатоканальний)
- +38 (093) 344-04-44 (багатоканальний)

26.4. Контактні дані з питань захисту персональних даних

З питань, пов'язаних із:

- захистом персональних даних;
- реалізацією прав суб'єктів персональних даних;
- конфіденційністю;
- міжнародним передаванням персональних даних;
- порушеннями безпеки персональних даних;
- виконанням вимог законодавства про захист персональних даних,

можна звертатися за адресою електронної пошти: **privacy@binotel.com**

26.5.Під час звернення рекомендується зазначити:

- тему звернення;
- контактні дані заявника;
- номер облікового запису або найменування організації (за наявності);
- короткий опис питання;
- документи або матеріали, необхідні для розгляду звернення.

26.6. Perevir може запросити додаткові відомості, необхідні для:

- підтвердження особи заявника;
- перевірки повноважень представника;
- уточнення змісту звернення;
- належного виконання вимог законодавства.

26.7.Звернення щодо персональних даних розглядаються відповідно до законодавства України, а якщо до відповідної обробки застосовується GDPR - також відповідно до вимог Регламенту (ЄС) 2016/679 (GDPR).

Додаток 1

Таблиця категорій персональних даних

Data Inventory Perevir

Цей Додаток є невіддільною частиною Політики конфіденційності Perevir та містить узагальнену інформацію про основні категорії персональних даних, які можуть оброблятися під час використання Системи.

Конкретний склад даних, мета, правова підстава, строк зберігання та роль Perevir залежать від:

- функціональності, яку використовує Користувач;
- типу облікового запису;
- умов договору;
- джерела отримання інформації;
- налаштувань корпоративного Користувача;
- застосовного законодавства;
- ролі Perevir у конкретній операції обробки.

Позначення ролей Perevir у таблиці:

- **володілець / контролер** - Perevir самостійно визначає мету та істотні засоби обробки;
- **розпорядник / процесор** - Perevir обробляє дані від імені корпоративного Користувача відповідно до його документованих вказівок;
- **технічний посередник** - Perevir забезпечує технічне отримання, передавання або відображення інформації з незалежного джерела;
- **одержувач** - Perevir законно отримує інформацію від іншого володільця, контролера або джерела;
- **змішана роль** - роль Perevir визначається окремо для різних операцій з однією категорією даних.

1. Узагальнена таблиця категорій персональних даних

№	Категорія даних	Суб’єкти даних	Приклади даних	Основні джерела	Основні цілі обробки	Правова підстава	Роль Perevir	Основні одержувачі	Орієнтовний строк зберігання
1	Реєстраційні дані облікового запису	Користувачі, адміністратори корпоративних облікових записів	ПІБ, електронна пошта, номер телефону, посада, організація, ідентифікатор облікового запису	Безпосередньо від Користувача або корпоративного клієнта	Реєстрація, створення та ведення облікового запису, комунікація, управління доступом	Укладення та виконання договору; законний інтерес; юридичний обов’язок	Володілець / контролер	Постачальники хостингу, електронної пошти, підтримки та безпеки	Протягом активності облікового запису та після його закриття протягом строку, необхідного для завершення розрахунків, розгляду претензій і виконання вимог законодавства
2	Дані автентифікації	Користувачі	Логін, криптографічний образ пароля, токени сесії, дані відновлення доступу, статус входу	Від Користувача та автоматично від Системи	Автентифікація, захист облікового запису, запобігання несанкціонованому доступу	Виконання договору; законний інтерес у забезпеченні безпеки	Володілець / контролер	Постачальники інфраструктури та інформаційної безпеки	До закриття облікового запису; окремі журнали та записи безпеки — протягом строку, визначеного політикою журналювання

3	Дані електронної ідентифікації	Користувачі, представники юридичних осіб	ПІБ, РНОКПП за наявності законної підстави, дані сертифіката КЕП, надавач довірчих послуг, результат перевірки, дата й час ідентифікації, ідентифікатор операції	КЕП, Дія.Підпис, кваліфіковані надавачі електронних довірчих послуг, державні системи	Підтвердження особи, повноважень, підписання документів, запобігання шахрайству	Виконання договору; юридичний обов’язок; законний інтерес; згода, коли вона необхідна	Володілець / контролер або технічний посередник	Надавачі електронних довірчих послуг, державні інформаційні системи, технічні адміністратори	Протягом строку, необхідного для підтвердження факту ідентифікації або юридично значущої дії, аудиту та захисту правових вимог
4	Дані корпоративного профілю та повноважень	Представники, працівники й адміністратори корпоративного Користувача	Найменування організації, код ЄДРПОУ, посада, роль, підрозділ, права доступу, статус адміністратора, довіреність або інше підтвердження повноважень	Від корпоративного Користувача, його представника, офіційних реєстрів	Управління корпоративним середовищем, визначення ролей і повноважень, виконання договору	Виконання договору; юридичний обов’язок; законний інтерес	Змішана роль	Уповноважені адміністратори клієнта, постачальники технічної інфраструктури	Протягом строку дії корпоративного облікового запису та необхідного після завершення договору періоду

5	Платіжні, договірні та бухгалтерські дані	Користувачі, представники клієнтів, платники, контактні особи	Платіжний статус, сума, дата, номер рахунку, акт, реквізити юридичної особи, дані платника, податкова інформація	Від Користувача, банку, платіжного провайдера, бухгалтерської системи	Проведення платежів, виставлення рахунків, бухгалтерський і податковий облік, повернення коштів	Виконання договору; юридичний обов'язок	Володілець / контролер	Банки, платіжні установи, бухгалтери, аудитори, податкові та інші уповноважені органи	Протягом строків, установлених податковим, бухгалтерським та архівним законодавством, а також строків позовної давності
6	Дані про використання Системи	Користувачі	Використані функції, дата й час дій, налаштування, переглянуті сторінки, створені звіти, активність у кабінеті	Автоматично під час використання Perevir	Надання функціональності, аналітика, підтримка, персоналізація, аудит, удосконалення Системи	Виконання договору; законний інтерес; згода для необов'язкової аналітики	Володілець / контролер	Постачальники хостингу, аналітики, моніторингу та підтримки	Протягом активності облікового запису або коротшого строку, визначеного для конкретної категорії технічних даних

7	Історія пошукових запитів	Користувачі та особи, щодо яких виконується пошук	Параметри пошуку, ПІБ, код ЄДРПОУ, РНОКПП за наявності підстави, номер справи, дата та результат запиту	Від Користувача та автоматично від Системи	Виконання запиту, історія перевірок, аудит, безпека, повторний доступ до результатів	Виконання договору; законний інтерес; документована вказівка клієнта	Змішана роль	Корпоративний Користувач, постачальники інфраструктури та безпеки	Протягом строку дії облікового запису, строку тарифу або строку, визначеного клієнтом; довше — для спору, аудиту чи безпеки
8	Реєстрові та офіційні дані	Керівники, засновники, бенефіціари, ФОП, сторони проваджень, інші особи, відомості про яких містяться у законних джерелах	ПІБ, статус, посада, корпоративні зв’язки, судові та виконавчі відомості, санкційні збіги, ліцензії, історія змін	Державні реєстри, офіційні системи, відкриті дані, ліцензовані постачальники	Інформаційний пошук, перевірка контрагентів, комплаєнс, моніторинг, формування звітів	Законодавчий дозвіл; законний інтерес; виконання договору; юридичний обов’язок Користувача	Технічний посередник, одержувач або процесор	Користувачі, корпоративні клієнти, постачальники інформаційних даних	Відображення в актуальному стані, кешування на обмежений строк або зберігання у звіті відповідно до умов функції

9	Дані третіх осіб, введені Користувачем	Працівники, кандидати, клієнти, контрагенти, представники, позичальники, поручителі та інші треті особи	ПІБ, контактні дані, ідентифікатори, коментарі, документи, відомості для перевірки	Від корпоративного Користувача, його працівників, API або інтеграцій	Виконання перевірки, комплаєнс, моніторинг, внутрішній облік, формування звітів	Правова підстава визначається корпоративним Користувачем	Переважно розпорядник / процесор	Корпоративний Користувач, уповноважені ним особи, погоджені постачальники	За вказівкою корпоративного Користувача, умовами DPA або до завершення договору з урахуванням обов'язкових строків
10	Завантажені документи та файли	Користувачі й особи, дані яких містяться у файлах	Таблиці, списки, документи, витяги, додатки, внутрішні коментарі, інші матеріали	Від Користувача, через API або інтеграцію	Обробка за завданням Користувача, аналіз, зберігання, формування звіту	Виконання договору; документована вказівка клієнта; інша підстава, визначена клієнтом	Розпорядник / процесор; в окремих випадках — контролер для безпеки	Корпоративний Користувач, постачальники хостингу, резервного копіювання й безпеки	До видалення Користувачем, завершення визначеної операції або припинення договору; резервні копії — до завершення технічного циклу
11	Сформовані звіти та результати перевірок	Особи, щодо яких сформовано звіт, і Користувачі, які його створили	Реєстрові відомості, історія змін, індикатори, збіги, висновки, дата формування, джерела	Дані Perevir, зовнішні джерела, параметри Користувача	Надання аналітичного результату, документування перевірки, повторне використання, аудит	Виконання договору; законний інтерес; документована вказівка клієнта	Змішана роль	Користувач, уповноважені особи клієнта, одержувачі, визначені самим Користувачем	Протягом строку, установленого тарифом, договором або налаштуваннями клієнта; до видалення чи знеособлення

12	Дані моніторингу	Суб’єкти, додані Користувачем до моніторингу	Ідентифікатори, контрольовані події, зміни статусу, сповіщення, дата перевірки	Від Користувача, державних та інших законних джерел	Регулярне відстеження змін, надсилання повідомлень, комплаєнс-контроль	Виконання договору; законний інтерес; юридичний обов’язок клієнта	Змішана роль	Корпоративний Користувач, постачальники реєстрових даних і комунікацій	До видалення суб’єкта з моніторингу, закриття облікового запису або припинення відповідної мети
13	Автоматично сформовані індикатори та аналітичні результати	Особи, щодо яких виконується перевірка, юридичні особи та пов’язані з ними фізичні особи	Індикатор ризику, категорія, бал, ймовірний збіг, зв’язок, аномалія, пояснення факторів	Реєстрові дані, дані Користувача, правила та аналітичні моделі Perevir	Структурування інформації, виявлення ознак і збігів, підтримка рішень Користувача	Виконання договору; законний інтерес; документована вказівка клієнта	Змішана роль	Користувачі та уповноважені особи корпоративного клієнта	Разом із відповідним звітом або протягом строку, установленого для конкретного аналітичного модуля
14	Технічні дані пристрою та з’єднання	Користувачі, відвідувачі вебсайту	IP-адреса, тип браузера, операційна система, пристрій, мова, часовий пояс, ідентифікатор сесії, URL, мережеві параметри	Автоматично від пристрою та мережі	Робота Системи, безпека, діагностика, аналітика, запобігання зловживанням	Законний інтерес; виконання договору; згода для необов’язкових технологій	Володілець / контролер	Постачальники хостингу, CDN, аналітики, моніторингу та кібербезпеки	Переважно протягом короткого технічного періоду; журнали безпеки можуть зберігатися довше відповідно до оцінки ризику

15	Журнали безпеки та аудиту	Користувачі, адміністратори, працівники, підрядники	Входи, невдалі спроби, IP-адреси, зміни ролей, адміністративні дії, експорти, API-запити, події безпеки	Автоматично від Системи та засобів безпеки	Контроль доступу, виявлення атак, розслідування інцидентів, аудит, доказування	Законний інтерес; юридичний обов'язок; захист правових вимог	Володілець / контролер	Постачальники кібербезпеки, аудитори, компетентні органи у встановлених законом випадках	Відповідно до типу журналу, критичності події, строку розслідування та строків правових вимог
16	Дані звернень до служби підтримки	Користувачі, контактні особи, заявники	ПІБ, контакти, зміст звернення, листування, вкладення, запис вирішення питання	Безпосередньо від заявника, корпоративного Користувача або через форму підтримки	Розгляд звернення, підтримка, контроль якості, доказування наданої консультації	Виконання договору; законний інтерес; юридичний обов'язок	Володілець / контролер або процесор залежно від змісту	Працівники підтримки, постачальники систем обробки звернень, консультанти	Протягом строку, необхідного для вирішення питання, контролю якості, спору та виконання законодавчих вимог
17	Дані звернень щодо персональних даних	Суб'єкти даних, їхні представники, заявники	Дані заявника, зміст вимоги, підтвердження особи, документи про представництво, відповідь і результат виконання	Безпосередньо від заявника або представника	Реалізація прав суб'єктів, виконання законодавства, документування дій	Юридичний обов'язок; законний інтерес у підтвердженні виконання вимог	Володілець / контролер	Відповідальні працівники, юридичні консультанти, корпоративний клієнт, наглядовий орган	Протягом строку розгляду звернення та надалі протягом строку, необхідного для підтвердження виконання й захисту правових вимог

18	Дані про порушення безпеки	Постраждалі суб’єкти, Користувачі, працівники, заявники	Опис події, категорії даних, журнали, наслідки, заходи реагування, контактні дані постраждалих	Системи моніторингу, Користувачі, працівники, постачальники, треті особи	Локалізація, розслідування, повідомлення, відновлення, запобігання повторенню	Юридичний обов’язок; законний інтерес; захист правових вимог	Володілець / контролер; процесор щодо клієнтських даних	Корпоративний клієнт, постачальники безпеки, консультанти, компетентні органи, постраждалі особи	До завершення розслідування та коригувальних дій, а також протягом строку, необхідного для аудиту й правових вимог
19	Cookies та аналогічні ідентифікатори	Користувачі та відвідувачі вебсайту	Ідентифікатор сесії, налаштування, інформація про згоду, аналітичний ідентифікатор, технічні параметри	Автоматично через браузер, вебсайт, SDK або аналогічну технологію	Автентифікація, збереження налаштувань, безпека, аналітика, маркетинг за наявності	Виконання договору; законний інтерес для необхідних cookies; згода для необов’язкових cookies	Володілець / контролер	Постачальники аналітики, хостингу, безпеки та комунікацій	Сесійні — до завершення сесії; постійні — до закінчення встановленого строку або відкликання згоди
20	Маркетингові та комунікаційні дані	Користувачі, потенційні клієнти, контактні особи	Ім’я, електронна пошта, номер телефону, мовні й комунікаційні налаштування, історія розсилок	Безпосередньо від особи, корпоративного клієнта або з іншого законного джерела	Надсилання новин, пропозицій, інформації про функції, проведення опитувань	Згода або законний інтерес у випадках, дозволених законом	Володілець / контролер	Постачальники електронної пошти, SMS, CRM та аналітики	До відкликання згоди, заперечення, втрати актуальності або завершення відповідної мети

21	Дані зворотного зв’язку та дослідження користуваць кого досвіду	Користувачі, представники клієнтів	Оцінки, коментарі, відповіді на опитування, пропозиції, інформація про роль і досвід використання	Безпосередньо від Користувача	Удосконалення продукту, оцінювання якості, планування функціональності	Законний інтерес; згода, якщо вона необхідна	Володілець / контролер	Постачальники опитувань, аналітики та продуктових досліджень	До завершення аналізу або довше у знеособленій чи агрегованій формі
22	Дані API та інтеграцій	Користувачі, адміністратори, особи, дані яких передаються через інтеграцію	API-ключі, технічні ідентифікатори, журнали запитів, передані поля, статуси обробки, помилки	Системи Користувача, партнерські API, Perevir	Забезпечення інтеграції, передавання даних, контроль доступу, діагностика, безпека	Виконання договору; документована вказівка клієнта; законний інтерес у безпеці	Змішана роль	Корпоративний клієнт, інтеграційні партнери, постачальники інфраструктури	Протягом дії інтеграції; журнали — протягом строку, необхідного для діагностики, безпеки й аудиту

2. Спеціальні категорії персональних даних

2.1. Perevir не призначений для систематичної обробки спеціальних категорій персональних даних, зокрема відомостей про:

- расове або етнічне походження;
- політичні переконання;
- релігійні чи світоглядні переконання;
- членство у професійних спілках;
- генетичні дані;
- біометричні дані, що використовуються для унікальної ідентифікації;

- стан здоров’я;
- статеве життя;
- сексуальну орієнтацію.

2.2.Обробка таких даних допускається лише тоді, коли одночасно:

- вона прямо необхідна для визначеної функції або законної мети;
- існує спеціальна правова підстава;
- обробка не заборонена застосовним законодавством;
- застосовано додаткові технічні й організаційні гарантії;
- обсяг даних обмежено мінімально необхідним;
- визначено спеціальний строк зберігання;
- за необхідності проведено оцінювання впливу на захист персональних даних.

2.3.Користувач не повинен завантажувати спеціальні категорії персональних даних без належної законної необхідності та погодженого сценарію обробки.

3. Дані про кримінальні правопорушення та судимості

3.1.У межах законної функціональності Perevir можуть оброблятися відомості про:

- кримінальні провадження;
- процесуальний статус особи;
- судові рішення;
- судимості;
- розшук;
- адміністративні правопорушення;
- санкції;
- виконавчі провадження;

- інші юридично значущі події.

3.2.Такі дані можуть використовуватися лише:

- за наявності належної правової підстави;
- для конкретної та законної мети;
- з дотриманням обмежень відповідного джерела;
- з урахуванням презумпції невинуватості;
- без автоматичного прирівнювання згадування у справі до встановленої вини;
- з додатковою перевіркою актуальності та контексту.

3.3.Процесуальний статус, наявність судової справи або збіг із записом не повинні самостійно використовуватися як доказ неправомірної поведінки особи.

4. Дані дітей

4.1. Perevir не призначений для створення облікових записів дітьми або систематичного формування профілів дітей.

4.2.Дані дітей можуть оброблятися лише у виняткових випадках, коли:

- це необхідно для законної мети;
- існує відповідна правова підстава;
- ураховані найкращі інтереси дитини;
- застосовані посилені заходи захисту;
- Користувач забезпечив законність такої обробки.

5. Категорії одержувачів

Персональні дані, залежно від конкретної операції, можуть передаватися таким категоріям одержувачів:

Категорія одержувача	**Мета доступу або передавання**
Постачальники хостингу та хмарної інфраструктури	Розміщення, обробка, резервне копіювання й забезпечення доступності Системи
Постачальники інформаційної безпеки	Виявлення загроз, моніторинг, захист від атак, розслідування інцидентів
Постачальники електронної ідентифікації	Перевірка КЕП, Дія.Підпису, сертифікатів і повноважень
Державні реєстри та їхні технічні адміністратори	Отримання або перевірка офіційної інформації
Комерційні постачальники інформаційних даних	Надання ліцензованих даних і доступу через API
Банки та платіжні установи	Проведення платежів, повернення коштів, запобігання шахрайству
Постачальники електронної пошти, SMS і повідомлень	Надсилання сервісних і дозволених маркетингових повідомлень
Постачальники аналітики та моніторингу	Оцінювання роботи Системи, діагностика помилок і продуктивності
Корпоративні Користувачі та їхні адміністратори	Управління корпоративним обліковим записом і використання результатів перевірок
Юридичні, бухгалтерські й аудиторські консультанти	Виконання законодавчих вимог, аудит і захист прав

Компетентні державні органи та суди	Виконання законних і належно оформлених вимог
Правонаступники або учасники корпоративної операції	Реорганізація, інвестиція, продаж бізнесу чи передавання активів за умови конфіденційності

6. Правові підстави обробки

Залежно від категорії даних і конкретної операції Perevir може використовувати одну або декілька таких правових підстав:

Правова підстава	**Приклади застосування**
Укладення або виконання договору	Реєстрація, доступ до Perevir, формування звіту, підтримка, оплата
Виконання юридичного обов’язку	Податковий і бухгалтерський облік, відповіді державним органам, зберігання документів
Законний інтерес	Захист Системи, запобігання шахрайству, журналювання, удосконалення продукту
Згода	Необов’язкові cookies, окремі маркетингові повідомлення, необов’язкові функції
Законодавчий дозвіл або повноваження	Використання відкритих даних, державних реєстрів, виконання спеціальної законодавчої процедури
Захист правових вимог	Зберігання доказів, розгляд претензій, судовий захист
Документована вказівка корпоративного Користувача	Обробка завантажених клієнтських даних у ролі процесора

Життєво важливі інтереси або суспільний інтерес	Лише у випадках, прямо передбачених і обґрунтованих законодавством

7. Критерії визначення строків зберігання

Якщо конкретний строк не встановлений у цій таблиці, договорі або законодавстві, Perevir визначає його з урахуванням:

- мети обробки;
- строку дії договору;
- активності облікового запису;
- вимог податкового, бухгалтерського та архівного законодавства;
- строків позовної давності;
- необхідності розслідування інцидентів;
- потреби у доказуванні юридично значущих дій;
- договірних вимог корпоративного Користувача;
- технічних циклів резервного копіювання;
- ризиків для прав і свобод суб’єктів;
- можливості знеособлення замість подальшого зберігання.

8. Міжнародне передавання

Окремі категорії персональних даних можуть оброблятися постачальниками, інфраструктура або персонал яких знаходяться за межами України.

У такому разі Perevir застосовує передбачені законодавством механізми, зокрема:

- перевірку належного рівня захисту;

- договірні гарантії;
- стандартні договірні положення, якщо застосовується GDPR;
- технічне шифрування;
- псевдонімізацію;
- мінімізацію переданих даних;
- обмеження віддаленого доступу;
- оцінювання ризиків міжнародного передавання.

9. Актуалізація Data Inventory

9.1.Адміністрація Perevir періодично переглядає цей Додаток у разі:

- запровадження нової функціональності;
- підключення нового джерела даних;
- залучення нового постачальника;
- зміни правової підстави;
- зміни строку зберігання;
- початку обробки нової категорії персональних даних;
- зміни ролі Perevir;
- виявлення нового ризику;
- зміни законодавства.

9.2.Внутрішній реєстр операцій обробки може містити детальнішу інформацію, ніж цей публічний Додаток, зокрема:

- найменування конкретної інформаційної системи;
- власника бізнес-процесу;
- структурний підрозділ;
- конкретного постачальника;
- країну розміщення;

- технічне місце зберігання;
- установлені строки видалення;
- класифікацію інформації;
- оцінку ризику;
- застосовані заходи безпеки;
- статус DPA;
- механізм міжнародного передавання;
- результати оцінювання впливу.

9.3.Зміни, які істотно впливають на права суб’єктів персональних даних, відображаються у новій редакції Політики конфіденційності або цього Додатку.