EWG CUSTOMS AGENCY

ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ

EWG Customs Agency Ltd.
Діє з: 30.08.2024.

Вступ

Закрите акціонерне товариство "EWG Customs Agency" (Реєстраційний номер: 01-10-141551; податковий номер: 27438635-2-41, надалі — Компанія або Контролер даних) зобов'язується захищати особисті дані своїх співробітників та ділових партнерів, а також третіх осіб, які вступають з нею в контакт, включаючи відвідувачів вебсайту https://ewgcustoms.com/ (надалі — Суб'єкти даних), і приділяє велику увагу дотриманню права на самовизначення. Ця Політика конфіденційності та, зокрема, правила та процедури, що містяться в ній, спрямовані на забезпечення того, щоб Контролер даних дотримувався чинних міжнародних та національних нормативно-правових актів, що стосуються захисту даних, зокрема Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року (надалі — "GDPR") та Закону CXII від 2011 року про право на інформаційне самовизначення та свободу інформації (надалі — "Інфо т.в."). Контролер даних діятиме відповідно до положень цієї Політики конфіденційності (надалі — "Політика конфіденційності") та інших внутрішніх правил і вказівок. Ця Політика конфіденційності переглядатиметься щорічно, і буде перевірено дотримання чинних правових норм. За зміст цієї Політики конфіденційності, її дотримання та правильне оформлення процесів відповідає керівництво.

Хто повинен дотримуватися цієї політики?

Співробітники Компанії, особи, які працюють в Компанії на інших умовах трудових відносин, та обробники даних, залучені Компанією, повинні дотримуватися цієї Політики та виконувати свою роботу відповідно до її положень.

ГОЛОВНІ ЗАКОНОДАВЧІ АКТИ

Контролер даних діятиме відповідно до наступних правових вимог при обробці даних, як це визначено в цій Політиці:

- Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний обіг таких даних, який скасовує Регламент (ЄС) № 95/46/ЄС (Загальний регламент про захист даних) (надалі — "GDPR")
- Закон CXII від 2011 року про право на інформаційне самовизначення та свободу інформації (надалі: Інфо т.в.)
- Закон V від 2013 року про Цивільний кодекс (надалі: Цивільний кодекс)
- Закон C від 2012 року про Кримінальний кодекс (надалі: Кримінальний кодекс)
- Закон I від 2012 року про Трудовий кодекс (надалі: Закон I від 2012 року про Трудовий кодекс)
- Закон XLI від 2012 року про Послуги з пасажирських перевезень (надалі: Закон про пасажирські перевезення)

- Закон CLV від 1997 року про захист прав споживачів (Фг. т.в.)
- Закон C від 2000 року про бухгалтерський облік (надалі: Закон про бухгалтерський облік)
- Закон LIII від 2017 року про запобігання та боротьбу з відмиванням грошей і фінансуванням тероризму (надалі: Пмт.)
- Закон CXXXIII від 2005 року про правила особистої та майнової охорони та приватного розслідування (надалі: Закон)

МЕТА КОДЕКСУ

Застосовуючи та дотримуючись правил, викладених у цій Політиці конфіденційності, Компанія може забезпечити практичну реалізацію положень чинного законодавства, зокрема GDPR, через внутрішні інструкції та процедури, засновані на цій Політиці конфіденційності. У цьому контексті Компанія встановлює за допомогою цієї Політики конфіденційності рамки, в межах яких:

- Забезпечується повага до основних прав Суб'єктів даних на захист персональних даних, а також дотримання та виконання вимог щодо безпеки даних;
- Регулюється процес планування, оцінки та перегляду ризиків, яким піддаються її дані;
- Регулюються практики запобігання несанкціонованому доступу до даних та встановлюються правила запобігання незаконним змінам, несанкціонованому використанню та несанкціонованому розголошенню даних;
- Визначаються точні та безпечні умови обробки, використання, передачі та знищення даних за допомогою електронних засобів;
- Встановлюються процедури та мінімальний зміст, необхідний для надання інформації суб'єктам даних та здійснення їх прав на інформацію;
- Встановлюються правила, яких слід дотримуватись у разі порушення безпеки персональних даних та в адміністративній процедурі;
- Визначаються мінімальні процедури, яких слід дотримуватися для підвищення обізнаності організації щодо захисту даних.

Детальні внутрішні інструкції та процедури повинні бути розроблені відповідно до цієї Політики конфіденційності, з урахуванням фактичних процесів та документовані за необхідності.

1. ЗАГАЛЬНА ЧАСТИНА

1.1. ТЛУМАЧЕННЯ ТЕРМІНІВ

Ознайомлення з поняттями при застосуванні правил:

- **"Персональні дані"** — будь-яка інформація, що стосується ідентифікованої або ідентифікувальної фізичної особи ("суб'єкт даних"); ідентифікувана фізична особа — це особа, яку можна ідентифікувати безпосередньо або опосередковано, зокрема за допомогою ідентифікатора, такого як ім'я, номер, дані про місцезнаходження, онлайн-

ідентифікатор або інші фактори, які належать до фізичної, фізіологічної, генетичної, психічної, економічної, культурної чи соціальної ідентичності цієї фізичної особи, тобто будь-які дані, завдяки яким можна ідентифікувати суб'єкта даних, такі як ім'я, адреса, телефонний номер, GPS-дані, IP-адреса тощо.

- **"Особливі категорії персональних даних"** — будь-які дані, що належать до особливих категорій персональних даних, а саме: персональні дані, що виявляють расове чи етнічне походження, політичні погляди, релігійні або філософські переконання, членство в профспілках, генетичні дані, біометричні дані, що дозволяють ідентифікувати фізичних осіб, медичні дані та персональні дані, що стосуються статевого життя або сексуальної орієнтації фізичних осіб.
- **"Обробка"** — будь-яка операція або набір операцій, що здійснюються з персональними даними або наборами персональних даних, незалежно від того, здійснюються вони автоматизованими чи неавтоматизованими засобами, такі як збирання, запис, організація, структуризація, зберігання, адаптація або змінення, пошук, консультація, використання, розкриття шляхом передачі, поширення або інше надання, об'єднання, обмеження, стирання або знищення — тобто будь-яка операція або набір операцій, що виконуються з даними, наприклад, запис, консультація, організація тощо.
- **"Передача"** — надання персональних даних визначеній третій особі.
- **"Розкриття"** — надання персональних даних будь-якій особі.
- **"Стирання"** — приведення персональних даних в такий стан, коли їх більше не можна відновити.
- **"Псевдонімізація"** — обробка персональних даних таким чином, що неможливо ідентифікувати фізичну особу, до якої ці персональні дані належать, без додаткової інформації, при цьому ця додаткова інформація зберігається окремо, і вживаються технічні та організаційні заходи, щоб забезпечити, що жодна ідентифікована чи ідентифікувальна особа не може бути пов'язана з цими персональними даними.
- **"Система файлів"** — набір персональних даних, організованих будь-яким чином, чи то централізовано, чи то децентралізовано, або структурований за функціональними чи географічними критеріями, доступний на основі визначених критеріїв.
- **"Інвентаризація даних"** — документ, що використовується для оцінки обсягу та характеру персональних даних, що обробляються контролером.
- **"Контролер"** — природна або юридична особа, орган публічної влади, агентство або будь-який інший орган, який, самостійно чи спільно з іншими, визначає цілі та засоби обробки персональних даних; якщо цілі та засоби обробки визначаються законодавством Союзу або держави-члена, контролер або конкретні критерії для призначення контролера можуть також визначатися законодавством Союзу або держави-члена; в цьому випадку контролером є Компанія.

- **"Обробник даних"** — природна або юридична особа, орган публічної влади, агентство або будь-який інший орган, який обробляє персональні дані від імені контролера; обробник даних — це особа чи підприємство, яке від імені та за вказівкою Компанії здійснює конкретні операції з персональними даними (надавач послуг з нарахування заробітної плати, постачальник хостингових послуг, постачальник програмного забезпечення, фахівець з охорони праці тощо).
- **"Отримувач"** — природна або юридична особа, орган публічної влади, агентство або будь-який інший орган, якому або з яким персональні дані передаються, незалежно від того, є він третім чи ні. Публічні органи, які можуть отримати доступ до персональних даних у контексті індивідуального розслідування відповідно до законодавства Союзу або держави-члена, не є отримувачами; обробка цих даних цими публічними органами повинна відповідати чинним правилам захисту даних відповідно до цілей обробки.
- **"Третя сторона"** — будь-яка природна або юридична особа, орган публічної влади, агентство або будь-який інший орган, окрім суб'єкта даних, контролера, обробника або осіб, які під безпосереднім контролем контролера або обробника мають дозвіл обробляти персональні дані.
- **"Третя країна"** — будь-яка країна, що знаходиться поза межами Європейської економічної зони.
- **"Згода суб'єкта даних"** — добровільне, конкретне, поінформоване та недвозначне вираження волі суб'єкта даних, яким він або вона підтверджує свою згоду на обробку персональних даних, що його стосуються, за допомогою заяви або однозначного акта підтвердження; це може бути письмова заява про згоду, ставлення галочки на вебсайті тощо; важливо зазначити, що з точки зору захисту даних мовчання не може бути визнано за згоду.
- **"Порушення персональних даних"** — порушення безпеки, яке призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, що передаються, зберігаються чи іншим чином обробляються; будь-яка подія, що ставить під загрозу дані, наприклад: атака хакерів, знищення архіву, втрата ноутбука, мобільного телефону, носія даних, надсилання персональних даних на неправильну електронну адресу, ненадійне зберігання даних (наприклад, квитанцій про оплату, що потрапляють в сміття), ненадійна передача даних, несанкціоноване копіювання списків клієнтів та їх партнерів тощо.
- **"Інцидент порушення конфіденційності"** — інцидент, що призводить до несанкціонованого або випадкового розкриття або доступу до персональних даних.
- **"Інцидент цілісності"** — інцидент, що призводить до несанкціонованої або випадкової зміни персональних даних.
- **"Інцидент доступності"** — інцидент, що призводить до несанкціонованої або випадкової втрати чи знищення персональних даних.

- **"Безпека даних"** — будь-які технічні або організаційні заходи, спрямовані на забезпечення безпеки оброблених персональних даних, фізичні, оптичні або організаційні, зокрема заходи для захисту від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження персональних даних.

1.2. ПРИНЦИПИ УПРАВЛІННЯ ДАНИМИ

Персональні дані

- обробка повинна бути законною, чесною та прозорою для суб'єкта даних ("законність, чесність і прозорість"); — це означає, що дані повинні оброблятися лише відповідно до відповідних правових положень, а суб'єкт даних повинен мати можливість бути належним чином проінформованим про обставини обробки (цілі, правова основа, тривалість тощо);
- збиратися повинні лише для визначених, чітких та законних цілей і не оброблятися способом, несумісним з цими цілями (додаткова обробка для архівних цілей в інтересах суспільства, наукових і історичних досліджень або статистичних цілей дозволена) ("обмеження мети"); — це означає, що дані, оброблені для визначеної мети, можуть використовуватися для інших цілей лише в виняткових випадках;
- повинні бути адекватними та релевантними для цілей, для яких вони обробляються, і обмежуватися лише тим, що є необхідним ("мінімізація даних"); — це означає, що персональні дані можуть оброблятися лише в тому випадку, якщо немає іншого способу досягти визначеної мети;
- повинні бути точними і, за потреби, актуальними; всі розумні заходи повинні бути вжиті, щоб забезпечити, що неточні для цілей обробки персональні дані були негайно стерті або виправлені ("точність"); — це означає, що зміни в даних повинні бути реалізовані якнайшвидше;
- повинні зберігатися в такій формі, яка дозволяє ідентифікацію суб'єкта даних тільки протягом того часу, який є необхідним для цілей, для яких персональні дані обробляються ("обмеження зберігання"); це означає, що після досягнення мети (максимальний період обробки) дані повинні бути стерті або анонімізовані так, щоб вони більше не могли бути використані для ідентифікації суб'єкта даних;
- повинні оброблятися таким чином, щоб забезпечити належний рівень безпеки персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження ("цілісність і конфіденційність"), з використанням відповідних технічних або організаційних заходів; — необхідні відповідні IT та інші заходи безпеки для запобігання несанкціонованому доступу до даних;
- Контролер несе відповідальність за дотримання вищезазначених принципів і має бути здатним продемонструвати таке дотримання ("підзвітність") — контролер повинен встановити свої процеси управління даними в внутрішніх інструкціях і політиках, щоб ці процеси могли бути точно виконані в організації (і, за необхідності, перевірені органами влади).

1.3. ЦІЛІ І ПРАВОВІ ОСНОВИ ОБРОБКИ

Цілі обробки даних

Ціль обробки визначається Компанією для кожної операції з обробки окремо перед початком обробки.

Загалом, ми обробляємо дані суб'єктів даних для цілей бізнесової діяльності Компанії, виконання договірних прав і зобов'язань.

Правова основа обробки даних

Правова основа для обробки також визначається Компанією для кожної окремої обробки.

Обробка персональних даних є законною лише тоді, коли виконується хоча б одна з таких умов:

а) Суб'єкт даних надав свою згоду на обробку своїх персональних даних для однієї чи кількох конкретних цілей:

Згода суб'єкта даних завжди є добровільною і може бути надана тільки через активний вчинок (мовчання не є згодою), наприклад, письмова згода (як у окремій заяві, так і, наприклад, підписанням контракту, де сам контракт містить згоду), позначення галочки в електронному інтерфейсі, натискання кнопки "Я погоджуюсь" тощо.

Згода повинна/може бути надана окремо для кожної операції обробки.

Суб'єкт даних має право відкликати свою згоду в будь-який час. Відкликання згоди не впливає на законність обробки на основі згоди, що мала місце до її відкликання, тобто згода може бути відкликана лише на майбутнє. Відкликання згоди повинно бути таким же легким, як і її надання, тобто воно може бути здійснене у вигляді письмового листа або заяви по телефону чи електронною поштою.

Згода особи, яка не досягла 16 років, або особи з обмеженою дієздатністю є дійсною, якщо її надає опікун/піклувальник особи, яка має батьківську опіку/обмежену дієздатність у випадку особи з батьківською опікою/обмеженою дієздатністю. У разі сумнівів вважається, що особа не надала свою згоду.

Згода суб'єкта даних вважається дійсною правовою основою для обробки, якщо це є вільно надана, конкретна, інформована і однозначна виявлена воля, якою суб'єкт даних виражає свою згоду на обробку персональних даних, що стосуються його/її особи, через заяву або дію, яка однозначно виражає його/її згоду на обробку.

Згода суб'єкта даних повинна гарантувати, що суб'єкт даних має реальний вибір і що не може бути сумнівів щодо "інформованості" цієї згоди.

Згода не вважається добровільною, якщо її наслідки підривають свободу вибору особи.

Крім того, за згодою суб'єкта даних:

- контролер повинен бути здатний продемонструвати, що суб'єкт даних надав свою згоду на обробку своїх персональних даних;
- контролер повинен забезпечити можливість суб'єкту даних відкликати згоду в будь-який час і повинен дозволити відкликання згоди таким же простим способом, як і надання згоди;
- мовчання, позначення галочки або бездіяльність не є згодою;
- згода не вважається наданою добровільно, якщо суб'єкт даних не має реального або вільного вибору і не може відмовити чи відкликати свою згоду без будь-яких наслідків;
- згода не вважається добровільною, якщо вона не дозволяє надання окремої згоди для різних операцій з обробки персональних даних;
- згода не може вважатися добровільною, якщо виконання контракту (наприклад, надання послуги) залежить від згоди на обробку, яка не є необхідною для виконання контракту;
- згода не буде дійсною правовою основою, якщо існує явна нерівність у відносинах між суб'єктом даних і контролером;
- коли контролер отримує згоду суб'єкта даних через письмову заяву, запит на згоду повинен бути чітко та однозначно відокремлений від решти контракту і повинен бути написаний чіткою і зрозумілою мовою контролером.

До отримання згоди контролер даних, особа, яка працює або має інше трудове або сервісне відношення з контролером даних, або обробник, що діє на основі договору з контролером, повинні надати суб'єкту даних відповідну інформацію. Інформація може бути надана за допомогою форми згоду, що спеціально для цього надається. В такому випадку суб'єкту даних має бути надано достатньо часу для ознайомлення з інформацією та її розуміння.

Суб'єкт даних має право запросити додаткову інформацію та роз'яснення від контролера даних, від особи, яка працює або має інше трудове відношення з контролером, або від обробника, який діє на основі договору з контролером. Надання інформації чи роз'яснення є обов'язковим.

(b) Обробка необхідна для виконання контракту, стороною якого є суб'єкт даних, або для цілей вжиття заходів на запит суб'єкта даних до укладання контракту (договірне зобов'язання): Якщо виконання контракту неможливе без обробки персональних даних, це може бути законною підставою для обробки. У таких випадках спеціальна згода суб'єкта даних не вимагається. Обробка даних у контексті виконання контракту найчастіше стосується персональних даних сторін контракту, які зазначені в контракті (ім'я, адреса тощо), але може також включати, наприклад, дані, що стосуються використання послуги. Це, наприклад, має місце, коли клієнту видається персоналізований рахунок під час покупки.

Персональні дані можуть бути оброблені з метою укладення контракту, якщо:

- контракт укладається Контролером даних із суб'єктом даних;
- суб'єкт даних надає дані Контролеру даних;
- дані необхідні для укладення контракту між Контролером даних і суб'єктом даних.

Персональні дані можуть бути оброблені для виконання контракту, якщо:

- є контракт, стороною якого є зацікавлена особа;
- контракт є дійсним;
- обробка насправді необхідна для досягнення загальної мети контракту.

Вимога необхідності є передумовою для застосування правової основи, що стосується контракту. Ця вимога не зводиться лише до аналізу умов контракту, але також передбачає розгляд гарантій захисту даних і принципів, викладених у GDPR, зокрема принципів справедливості, обмеження цілей і мінімізації даних. Таким чином, якщо обробка є корисною, але не об'єктивно необхідною для виконання контракту, правова основа контракту не застосовується.

(c) обробка необхідна для виконання правових зобов'язань, які покладаються на Контролера даних (правове зобов'язання)

Виконання правового зобов'язання може бути правовою основою для обробки персональних даних, якщо:

- це вимагається законодавством ЄС або національним правом;
- положення містить обов'язок, що прямо застосовний до Контролера даних;
- положення служить загальним інтересам;
- положення пропорційне до законної мети, що переслідується.

Метою обробки на підставі законодавства є виконання зобов'язань, встановлених цим законодавством. Законодавчо обов'язкова обробка вважається обов'язковою, обсяг і тривалість якої завжди визначаються відповідним законодавством. Велика кількість законів накладає обов'язок обробляти дані. Важливо зазначити, що правові зобов'язання не є факультативними і повинні завжди виконуватися. Наприклад, обробка даних щодо податкових зобов'язань, нарахування заробітної плати, обробка даних щодо обов'язкових атестаційних тестів, записи в управлінні претензіями за гарантією тощо.

(d) Обробка, коли обробка необхідна для захисту життєвих інтересів суб'єкта даних або іншої фізичної особи

У конкретному випадку, коли суб'єкт даних не може самостійно здійснювати свої інтереси або йому заважають це зробити, можливе забезпечення обробки його даних лише в межах, необхідних для захисту життєвих інтересів, і лише на період перешкоди.

(e) Обробка, коли обробка необхідна для виконання завдання, що здійснюється в публічному інтересі або в рамках здійснення публічної влади, наданої контролеру (обробка в межах публічної влади).

Компанія не є публічним органом і не здійснює обробку даних на такій правовій основі.

(f) Обробка, коли обробка необхідна для цілей законних інтересів, що переслідуються контролером або третім суб'єктом (законний інтерес), за умови, що ці інтереси не перевищують інтереси або основні права та свободи суб'єкта даних, що вимагають захисту персональних даних, зокрема коли суб'єкт даних є дитиною.

Законні інтереси контролера, включаючи контролера, з яким можуть бути передані персональні дані, або третю сторону, можуть бути правовою основою для обробки, якщо інтереси, основні

права та свободи суб'єкта даних не переважають законні інтереси контролера, враховуючи розумні очікування суб'єкта даних на основі його відносин з контролером.

Законний інтерес контролера, включаючи контролера, з яким можуть бути передані персональні дані, або третьої сторони, не є правовою основою для обробки, коли обробка здійснюється контролером або третьою стороною в контексті виконання публічного завдання.

Для встановлення наявності законного інтересу необхідно врахувати, зокрема, чи міг суб'єкт даних розумно очікувати, під час збору персональних даних, що обробка для вказаних цілей відбудеться.

Інтереси та основні права суб'єкта даних можуть переважити інтереси контролера, якщо персональні дані обробляються в умовах, коли суб'єкти даних не очікують подальшої обробки.

Обробка на основі законного інтересу як правова підстава вимагає від Контролера даних проведення так званого тесту балансування інтересів. Тест балансування інтересів складається з наступних етапів:

- необхідно встановити законний, чіткий і актуальний інтерес контролера;
- визначити основні права та свободи суб'єкта даних, врахувати очікування суб'єкта даних;
- проаналізувати необхідність і пропорційність обробки;
- слід вжити додаткових заходів для зменшення впливу обробки даних.

У всіх випадках компанія повинна документувати тест інтересів в письмовій формі, і суб'єкт даних може запросити інформацію про будь-яке припинення проведення тесту інтересів.

Тест оцінки інтересів детально описано в розділі 2.1.

1.4. ПРАВА СУБ'ЄКТІВ ДАНИХ У ЗВ'ЯЗКУ З ОБРОБКОЮ ДАНИХ

Вимога попереднього інформування

Під час отримання персональних даних суб'єкт даних повинен бути проінформований про факт їх обробки, мету, правову основу, обсяг оброблюваних даних, метод, тривалість або критерії визначення тривалості обробки, правила щодо портативності даних, а також право подати скаргу до наглядового органу.

Окрім зазначеної інформації, суб'єкт даних повинен бути чітко поінформований про можливість реалізації права на заперечення, і ця інформація повинна бути окремо виділена від будь-якої іншої інформації.

Інформація:

(a) повинна бути надана кандидатам на сторінці, де опубліковано оголошення про вакансію, відповідно до відповідного повідомлення про обробку даних;

(b) особам, які встановлюють трудові відносини або інші трудові відносини з контролером даних, на момент встановлення правовідносин, з вмістом відповідної інформації щодо обробки даних;

Інформація, зазначена в пункті (a), повинна бути доступною на вебсайті контролера даних у

стислому, прозорому та легкодоступному вигляді, зрозумілою та чіткою мовою. Інформація, зазначена в пункті (b), повинна бути надана в електронному вигляді на момент встановлення правовідносин, і особа, на яку це стосується, повинна надати письмове підтвердження цього у вигляді паперової заяви.

Право на доступ суб'єкта даних

На вимогу суб'єкта даних компетентний адміністратор, відповідальний за обробку, має надати інформацію про поточну обробку персональних даних суб'єкта даних протягом 30 днів з моменту отримання запиту.

Суб'єкт даних має право на доступ до своїх персональних даних та наступної інформації:

a) мети обробки;

b) категорії персональних даних, що обробляються;

c) отримувачі або категорії отримувачів, яким були або будуть розкриті персональні дані, зокрема отримувачі в третіх країнах або міжнародних організаціях;

d) у разі застосування, передбачений період зберігання персональних даних або, якщо це неможливо, критерії для визначення цього періоду;

e) право суб'єкта даних отримати від контролера виправлення, видалення або обмеження обробки персональних даних, що стосуються нього, а також заперечувати проти обробки таких персональних даних;

f) право подати скаргу до наглядового органу;

g) якщо дані не були зібрані від суб'єкта даних, будь-яка доступна інформація щодо їх джерела.

Доступ до персональних даних має бути забезпечений таким чином, щоб суб'єкт даних, наскільки це можливо, не дізнався про персональні дані іншої особи. Виняток може бути зроблений для персональних даних, які стосуються як суб'єкта даних, так і іншої особи.

Контролер даних може обмежити або відмовити в праві доступу суб'єкта даних пропорційно до мети, яку він переслідує, якщо така міра є строго необхідною:

a) для ефективного і результативного проведення розслідувань або проваджень, що стосуються контролера даних, зокрема кримінальних розслідувань;

b) для ефективного і результативного запобігання та виявлення кримінальних правопорушень; c) для виконання покарань і заходів проти правопорушників;

d) для ефективного і результативного захисту громадської безпеки;

e) для ефективного і результативного захисту зовнішньої та внутрішньої безпеки держави, зокрема національної оборони та національної безпеки;

f) для забезпечення захисту основних прав третіх осіб.

Якщо контролер даних відмовляє або обмежує право суб'єкта даних на доступ, як зазначено вище, контролер зобов'язаний негайно письмово повідомити суб'єкта даних, зазначивши причини застосування цього заходу, за умови, що мета обмеження або відмови не буде поставлена під загрозу. У повідомленні контролер має спеціально звернути увагу суб'єкта даних на те, що він або вона може реалізувати своє право на доступ за допомогою наглядового органу.

Контролер даних має вести облік своїх дій стосовно реалізації права на доступ у реєстрі, що додається до Правил. Якщо контролер обмежує або відмовляє у праві доступу, він зобов'язаний вказати юридичні та фактичні причини для такого заходу.

Право на виправлення

Суб'єкт даних має право на отримання від контролера, на його вимогу та без невиправданої затримки, виправлення неточних персональних даних, що стосуються його чи її. Зважаючи на мету обробки, суб'єкт даних має право на отримання виправлення неповних персональних даних, у тому числі шляхом додаткової декларації.

На вимогу суб'єкта даних компетентний адміністратор, відповідальний за обробку даних, повинен без невиправданої затримки виправити неточні персональні дані, що стосуються суб'єкта даних. Зважаючи на мету обробки, суб'єкт даних також має право на запитання про доповнення неповних персональних даних, включаючи додаткову декларацію.

Будь-який отримувач, якому або з яким були розкриті персональні дані, має бути проінформований про зміну, якщо це не є неможливим або не передбачає непропорційних зусиль. Суб'єкт даних може отримати інформацію про таких отримувачів за запитом.

Право на стирання ("право бути забутим")

Суб'єкт даних має право на отримання від контролера стирання персональних даних, що стосуються його чи її, без невиправданої затримки на вимогу, і контролер зобов'язаний без невиправданої затримки стерти персональні дані, якщо виконано хоча б одну з таких умов:

- персональні дані більше не потрібні для цілей, для яких вони були зібрані або іншим чином оброблені (мета обробки була виконана);
- суб'єкт даних відкликає згоду, на основі якої відбувалась обробка, і не існує іншої правової основи для обробки;
- правова основа для обробки — це законний інтерес контролера, і суб'єкт даних заперечує проти обробки, і немає переважаючих законних підстав для обробки, або суб'єкт даних заперечує проти обробки з метою прямого маркетингу;
- персональні дані були незаконно оброблені;
- персональні дані повинні бути стерті для виконання юридичного зобов'язання, що накладається законодавством ЄС або країни-члена, що застосовується до контролера (наприклад, якщо цього вимагає державний орган).

Якщо контролер розкрив персональні дані і зобов'язаний їх видалити згідно з вищезазначеним, він повинен вжити розумних заходів, включаючи технічні засоби, враховуючи доступні технології та витрати на їх впровадження, для інформування інших контролерів, що обробляють ці дані, про те, що суб'єкт даних запитав видалення посилань на або копій чи реплік персональних даних.
Контролер не зобов'язаний видаляти дані, якщо обробка є необхідною для:

- здійснення права на свободу вираження думки та інформації;
- виконання юридичного зобов'язання, що вимагає від контролера обробки персональних даних;
- у певних випадках з підстав публічного інтересу в галузі охорони здоров'я;
- для архівування в публічних інтересах, наукових і історичних досліджень або статистичних цілей, де видалення даних може значно ускладнити або зашкодити досягненню цієї мети;
- для пред'явлення, захисту або відстоювання юридичних вимог.

Усі отримувачі, яким або з якими були розкриті персональні дані, повинні бути поінформовані про видалення, якщо це не є неможливим або не передбачає непропорційних зусиль. Суб'єкт даних може отримати інформацію про таких отримувачів за запитом.

Право на обмеження обробки

Суб'єкт даних має право отримати від контролера обмеження обробки, якщо виконано хоча б одну з наступних умов:

- суб'єкт даних оскаржує точність персональних даних, у такому випадку обмеження застосовується на період часу, необхідний для перевірки точності персональних даних (тобто поки не буде встановлено, що оброблювані дані є точними);
- обробка даних є незаконною, але суб'єкт даних проти їх видалення та замість цього запитує обмеження їх використання (оскільки обробка даних може стати законною, і дані не треба буде заново записувати);
- контролер більше не потребує персональних даних для цілей обробки, але суб'єкт даних вимагає їх для встановлення, здійснення або захисту юридичних вимог;
- суб'єкт даних заперечує проти обробки на підставі законного інтересу; у цьому випадку обмеження застосовується до періоду, поки не буде встановлено, чи переважають законні підстави контролера над підставами суб'єкта даних.

Якщо обробка даних обмежена, згідно з наведеними вище умовами, такі персональні дані можуть оброблятися, за винятком зберігання, лише за згодою суб'єкта даних або для встановлення, здійснення або захисту юридичних вимог чи для захисту прав іншої фізичної або юридичної особи, або для важливих публічних інтересів. Суб'єкт даних має бути проінформований про зняття обмеження на обробку.

Будь-який отримувач, якому або з яким були розкриті персональні дані, повинен бути проінформований про обмеження обробки, якщо це не є неможливим або не передбачає непропорційних зусиль. Суб'єкт даних має право отримати інформацію про таких отримувачів за запитом.

Право на перенесення даних

На вимогу суб'єкта даних компетентний адміністратор, відповідальний за обробку, забезпечить перенесення персональних даних за умови, що виконуються наступні умови:

a) персональні дані були надані суб'єктом даних контролеру;

b) правова основа для обробки є згода або контракт між суб'єктом даних і контролером;

c) обробка здійснюється автоматизованими засобами;

d) обробка персональних даних не шкодить правам або свободам інших осіб.

При реалізації права на перенесення даних контролер надасть персональні дані суб'єкту даних у структурованому, широко використовуваному, машинозчитуваному форматі (PDF/XML). Суб'єкт даних має право вимагати, щоб контролер передав персональні дані безпосередньо іншому контролеру. Суб'єкт даних може реалізувати цей варіант тільки в разі, якщо це технічно можливо. Контролер також зобов'язаний надати персональні дані на папері для полегшення реалізації права на доступ.

Право на заперечення

Суб'єкт даних має право в будь-який час, з огляду на його чи її конкретну ситуацію, заперечувати проти обробки персональних даних, що здійснюється в публічних інтересах або на основі законних інтересів компанії, включаючи профілювання на основі зазначених положень. У такому випадку контролер більше не має права обробляти персональні дані, якщо не продемонструє переконливі законні підстави для обробки, які переважають інтереси, права та свободи суб'єкта даних або для встановлення, здійснення чи захисту юридичних вимог.

Якщо персональні дані обробляються для цілей прямого маркетингу (наприклад, маркетинг, розсилка новин тощо), суб'єкт даних має право в будь-який час заперечувати проти обробки своїх персональних даних для таких цілей, включаючи профілювання, якщо воно пов'язане з прямим маркетингом.

Якщо суб'єкт даних заперечує проти обробки персональних даних для цілей прямого маркетингу, персональні дані більше не можуть оброблятися для цих цілей.

Право подати скаргу до наглядового органу

Не порушуючи інших адміністративних або судових засобів правового захисту, кожен суб'єкт даних має право подати скаргу до наглядового органу, зокрема в країні його або її звичайного місця проживання, місця роботи або місця порушення, якщо суб'єкт даних вважає, що обробка персональних даних, що стосуються його або її, порушує положення GDPR.

Наглядовий орган має розслідувати суть скарги та повідомити скаржника про результати розслідування в розумний термін, зокрема якщо необхідно провести подальше розслідування або співпрацювати з іншими наглядовими органами. Після подачі скарги наглядовий орган має право ініціювати процедуру проти контролера.

Якщо контролер не вживає заходів щодо запиту суб'єкта даних, він зобов'язаний без затримки, але не пізніше ніж через місяць після отримання запиту, поінформувати суб'єкта даних про причини невиконання запиту та можливість подати скаргу до наглядового органу і реалізувати своє право на судовий захист.

Точні контактні дані угорського наглядового органу вказані в Політиці конфіденційності.

Обмеження

Законодавство ЄС або країни-члена, яке застосовується до контролера або обробника, може в деяких випадках обмежувати права суб'єктів даних, як зазначено вище, через законодавчі заходи.

2. ПРОЦЕДУРНІ ІНСТРУКЦІЇ

2.1. Тест балансування інтересів

У всіх випадках, коли правовою підставою для обробки є законний інтерес Компанії, має бути проведено тест балансування інтересів, і результат цього тесту повинен бути належним чином задокументований. Форма для тесту балансування інтересів додається як Додаток 1 до цих Інструкцій з обробки даних.

2.1.1. Кроки тесту балансування інтересів

1. Крок 1: Визначення мети обробки

Персональні дані можуть бути оброблені лише для заздалегідь визначених, законних цілей. Так звана "накопичувальна" обробка, коли дані збираються для непередбаченої мети, заборонена. Мета обробки має бути чітко та зрозуміло визначена.

2. Крок 2: Чітке визначення законного інтересу

Законні інтереси, що використовуються як правова підстава для обробки, повинні бути визначені точно і ясно, достатньо детально, щоб бути сумісними з основними правами та свободами суб'єктів даних. Законний інтерес має бути інтересом, який переслідується контролером і є актуальним для його поточної діяльності. Занадто загальні або теоретичні інтереси не є прийнятними.

Зокрема, законний інтерес:

- має бути законним (тобто відповідати вимогам законодавства ЄС та/або національного законодавства);
- має бути достатньо чітким (тобто достатньо точним), щоб можна було провести тест балансування інтересів щодо інтересів і основних прав суб'єктів даних;
- має бути реальним і наявним інтересом (тобто не теоретичним).

Законним інтересом є, зокрема:

- пряма реклама, маркетингові дослідження;
- правові претензії, включаючи стягнення претензій за позасудовими процедурами;
- запобігання шахрайству, зловживанню послугами або відмиванню грошей;
- перевірки працівників;
- забезпечення фізичної, IT та мережевої безпеки.

3. Крок 3: Визначення того, чи є обробка строго необхідною для досягнення цілей інтересу

Цей крок передбачає оцінку того, чи можна досягти мети обробки без обробки даних. Якщо це можливо, обробка є непотрібною, і її не можна здійснювати. Якщо мета не може бути досягнута без обробки, то тест балансування інтересів можна продовжувати.

4. Крок 4: Оцінка, чи переважають інтереси контролера над основними правами або інтересами суб'єктів даних

Для визначення цього слід врахувати такі обставини:

- характер інтересу контролера (основне право, публічний інтерес, законне право, комерційний інтерес);
- шкода, яку понесе контролер, треті особи або широка спільнота в разі відмови в обробці;
- характер даних (конфіденційні або чутливі в широкому розумінні);
- правовий статус суб'єктів даних (неповнолітні, працівники тощо) та контролера (наприклад, чи має компанія домінуючу ринкову позицію);
- спосіб обробки даних (профілювання, вплив на велику кількість осіб);
- основні права та/або інтереси суб'єктів даних, які можуть бути порушені;
- розумні очікування зацікавлених сторін;
- порівняння ефектів для суб'єктів даних з вигодами для контролера від обробки.

Загальний огляд: оцінка, чиї інтереси є більш важливими і чому

1. Крок 3: Підготовка підсумкової таблиці балансу з урахуванням додаткових гарантій

Необхідно визначити заходи для зменшення потенційного впливу обробки даних:

- Мінімізація даних (обробляються тільки дані, які є строго необхідними, і ці дані повинні бути видалені одразу після досягнення мети, функція видалення повинна бути автоматизована, якщо це можливо);
- Впровадження технічних і організаційних заходів, щоб забезпечити, що дані не можуть бути використані для прийняття рішень щодо осіб або для інших дій (функціональна ізоляція);
- Широке використання технік анонімізації, агрегації даних, технологій, що забезпечують конфіденційність;
- Право на заперечення (опція відмови).

2. Крок 4: Забезпечення прозорості - документування рішення

- Процес тесту балансування інтересів, обставини, що враховуються на кожному етапі, має бути задокументовано в достатньо детальній формі для того, щоб продемонструвати, що рішення є обґрунтованим.
- У разі сумнівів необхідно залучати офіцера з захисту даних/експерта.
- Якщо обробка даних несе високий ризик для прав і свобод суб'єктів даних, повинна бути проведена оцінка впливу на захист даних.

2.1.2. Результати тесту оцінки інтересів

Тест оцінки інтересів має бути проведений для всіх діяльностей з обробки даних у Компанії, де законним основанням для обробки є законний інтерес Компанії. Процес балансування інтересів повинен охоплювати всі специфікації діяльності Компанії.

Усі тести оцінки інтересів повинні бути документовані письмово.

Інформаційне повідомлення про управління даними повинно надавати просту, чітку та прозору інформацію суб'єктам даних щодо результатів тесту оцінки інтересів.

2.1.3. Огляд тесту балансування інтересів

Висновки тесту балансування інтересів повинні переглядатися принаймні раз на рік, а також у разі зміни обставин управління даними.

Крім того, у разі заперечення суб'єкта даних щодо обробки, тест балансування інтересів повинен бути переглянутий для конкретного суб'єкта даних, з урахуванням його чи її індивідуальних обставин, і результати перегляду тесту балансування інтересів повинні бути повідомлені суб'єкту даних при розгляді заперечення.

2.2. ОЦІНКА РИЗИКІВ І ОЦІНКА ВПЛИВУ НА ЗАХИСТ ДАНИХ

Оцінка ризиків захисту даних та оцінка впливу на захист даних надають рішення щодо того, як визначити потенційні ризики для кожної операції з обробки даних і, за необхідності, як провести оцінку впливу на захист даних та як керувати ризиками.

Національний орган захисту даних оприлюднив позицію, що стосується того, які діяльності підлягають обов'язковій оцінці впливу на захист даних. Актуальний список доступний на сайті НЦА і має бути перевірений при плануванні кожної операції з обробки даних.

Процес оцінки ризиків і оцінки, як і всі подібні процеси, вимагає раціонального підходу та повного розуміння загальних цілей, які полягають у захисті персональних даних у максимальному обсязі та у відповідності з вимогами GDPR.

Згідно з GDPR, неспроможність виконати вимоги щодо оцінки впливу на захист даних призведе до накладення штрафу на контролюючий орган. Несвоєчасне проведення оцінки впливу на захист даних у випадках, коли це є обов'язковим (стаття 35(1) та (3-4)), неповне виконання оцінки впливу на захист даних (стаття 35(2) і (7), (9)) та неналежне консультування з наглядовим органом зазнають штрафу, який може становити до €10 млн або 2% від загального річного обороту компанії за попередній фінансовий рік, залежно від того, яка сума більша.

Діаграма процедури оцінки ризиків додається як Додаток 2 до цих Інструкцій із захисту даних.

2.2.1. Визначення необхідності та обставин

Відповідно до ризикового підходу, передбаченого GDPR, оцінка впливу не є обов'язковою для кожної окремої операції з обробки даних. Оцінка впливу вимагається лише у випадках, коли обробка персональних даних може створювати "високий" ризик для прав і свобод фізичних осіб (стаття 35(1) GDPR). Той факт, що умови для обов'язковості проведення оцінки впливу не виконуються, не зменшує загальну обов'язок вживати необхідні заходи для виявлення та адекватного реагування на ризики для прав і свобод суб'єктів даних, що є частиною оцінки ризиків. На практиці це означає, що ризики, що виникають внаслідок діяльності з обробки персональних даних, повинні оцінюватися на постійній основі.

Оцінка впливу на захист даних/оцінка ризиків повинна проводитися до початку обробки і є інструментом прийняття рішень для обробки.

Оцінку впливу на захист даних/оцінку ризиків слід починати якомога раніше при проектуванні операцій з обробки даних, навіть якщо деякі операційні елементи ще не відомі. Постійне адаптування оцінки впливу на захист даних/оцінки ризиків протягом життєвого циклу проекту забезпечить належний захист даних та сприятиме рішенням, що полегшують дотримання вимог GDPR.

Якщо процес розробки триває, може бути необхідним повторення деяких етапів оцінки, оскільки певні технічні чи організаційні заходи можуть вплинути на серйозність або ймовірність ризиків, пов'язаних з управлінням даними. Оцінка впливу/оцінка ризиків є постійною обов'язковою процедурою, особливо в тих випадках, коли операції з управління даними підлягають динамічним змінам.

Те, що процедура оцінки впливу/оцінка ризиків може потребувати змін після фактичного початку обробки даних, не є достатньою підставою для відкладення чи припинення оцінки. Таким чином, оцінка впливу/оцінка ризиків — це не одноразова задача, а постійне завдання.

Низка умов має бути врахована для визначення того, чи зобов'язана Компанія проводити оцінку впливу на захист даних.

Згідно з GDPR (стаття 35), оцінка впливу вимагається зокрема у випадках, коли передбачена обробка може включати:

- Систематичну та масштабну оцінку певних аспектів персональних даних, що стосуються фізичних осіб на основі автоматизованої обробки, включаючи профілювання, і на основі яких приймаються рішення, що мають юридичні наслідки для фізичної особи або подібним чином істотно впливають на неї (наприклад, систематичний моніторинг діяльності працівників, включаючи їх місце роботи, інтернет-активність тощо);
- Обробку спеціальних категорій персональних даних, зазначених у статті 9(1) або обробку великої кількості персональних даних щодо рішень, що стосуються кримінальної відповідальності та порушень, зазначених у статті 10;

- Масштабне, систематичне спостереження за публічними місцями (наприклад, збір даних із соціальних мереж для створення профілів).

Примітка: Стаття 9(1) стосується обробки персональних даних, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, членство в профспілках, генетичні дані, біометричні дані для цілей унікальної ідентифікації фізичних осіб, дані про здоров'я та дані щодо статевого життя або сексуальної орієнтації фізичних осіб.

Вищезазначений список не є вичерпним, і в залежності від обставин можуть бути й інші діяльності з обробки даних "високого" ризику, які не включені в цей список.

Загалом, Компанія буде визначати, чи необхідна оцінка впливу на захист даних для певного проекту, зважаючи на список, опублікований НЦА, та на наявність одного чи кількох із таких умов: a) персональні дані надаються особам або організаціям, які раніше не мали до них доступу; b) персональні дані, які вже обробляються, використовуються для інших цілей або іншими способами; c) буде впроваджена нова технологія управління даними; d) автоматизоване прийняття рішень/профілювання.

Якщо не ясно, чи необхідна оцінка впливу на захист даних для певного проекту, рекомендується провести її. У разі необхідності можна звернутися до DPO (якщо такий є) для уточнення, також можна звернутися до органу захисту даних. У всіх випадках керівництво має право та обов'язок прийняти рішення (за допомогою експертів) про те, чи потрібно проводити оцінку впливу, чи слід звертатися до органу захисту даних.

2.2.1 Повний контекст проведення оцінки впливу та пояснення причин для оцінки

Повний контекст, у якому була проведена оцінка впливу, а також пояснення причин проведення цієї оцінки повинні бути задокументовані. Пояснення повинно включати як внутрішній, так і зовнішній контекст проєкту та його основні цілі.

- Обсяг дослідження також має бути чітко визначений, що може бути виражено через конкретні обставини проєкту, зокрема:
- Географічне розташування: наприклад, країна, офіс, дата-центр.
- Організаційні підрозділи: наприклад, конкретні відділи.
- Бізнес-процес: причина або ціль.
- IT-послуги, системи чи мережі: опис залучених IT-послуг, систем чи мереж.
- Клієнти, продукти чи послуги: опис клієнтів, продуктів чи послуг, що стосуються проєкту.

Будь-яке виключення повинно бути детально обґрунтоване.

2.2.2 Документування використання персональних даних

Відповідно до статті 35(7)(a) та (b) Регламенту GDPR, оцінка впливу повинна містити щонайменше:

a) систематичний опис передбачених операцій з обробки та опис цілей обробки, включаючи, де це необхідно, законні інтереси, які переслідує контролер;

b) оцінку необхідності та пропорційності операцій з обробки з урахуванням цілей обробки.

Необхідно продемонструвати та задокументувати в достатній деталізації, що персональні дані, які використовуються в проєкті, є релевантними, враховуючи такі аспекти:

- Визначення окремих елементів даних, які зберігаються та обробляються.
- Причини, чому обробка є абсолютно необхідною та пропорційною.
- Мета та правова підстава обробки.
- Як були отримані дані (джерело даних).
- Як обробляються дані (операції обробки, операції, виконувані процесорами).
- Тривалість обробки даних.
- Як і де зберігаються дані.
- Можливе подальше використання даних.
- Передача даних.
- Доступ до даних.

Інформацію можна збирати та представляти через відповідні реєстри інформації, блок-схеми та інструменти доступу до даних.

2.2.3 Ідентифікація ризиків

Ідентифікація ризиків, пов'язаних з персональними даними, які збираються, обробляються та зберігаються, включає кілька етапів:

2.2.3.1 Ідентифікація джерел ризиків

Для ідентифікації ризиків слід проконсультуватися з наступними особами:

- Менеджери, відповідальні за відповідні діяльності.
- Персонал, який фактично здійснює діяльність.
- Постачальники послуг, відповідальні за надання вхідних даних для діяльності.
- Особи, які отримують результати діяльності.
- Треті особи, що мають відповідні знання щодо діяльності.
- Представники осіб/організацій, що надають підтримку та ресурси для діяльності.
- Інші особи, які можуть корисно сприяти процесу ідентифікації ризиків.

Всі виявлені ризики повинні бути зафіксовані в максимально можливих деталях для подальшої оцінки ймовірності та впливу цих ризиків.

2.2.4 Аналіз ризиків

Ризики для прав і свобод суб'єктів даних, різної ймовірності та складності, можуть виникати внаслідок обробки персональних даних, що може призвести до фізичних, матеріальних або нематеріальних збитків. Зокрема, обробка може призвести до:

- дискримінації,
- крадіжки або шахрайства з ідентичністю,
- фінансових втрат,
- шкоди репутації,

- порушення конфіденційності персональних даних, захищених професійною таємницею,
- надмірного впливу на бізнес-рішення,
- несанкціонованого видалення псевдонімізації,
- інших значних економічних чи соціальних збитків.

Шкода може виникати різними способами. Іноді вона може бути відчутною та кількісно визначеною, такою як фінансові втрати чи втрата роботи. В інших випадках шкода менш визначена, наприклад, шкода, спричинена витоком конфіденційної чи чутливої інформації в особисті стосунки та соціальні ситуації. Іноді шкода не є очевидною, такою як страх перед крадіжкою особистих даних, що може призвести до компрометації інформаційної безпеки. Шкода, що виникає від використання персональної інформації, може бути непомітною для осіб і не мати наслідків.

Ймовірність і серйозність ризику для прав і свобод суб'єктів даних повинні визначатися з урахуванням цілей, характеру, обсягу та обставин обробки.

При оцінці ризиків для безпеки даних слід враховувати ризики, пов'язані з обробкою персональних даних, такі як випадкове чи незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних, або передача, зберігання чи інша обробка персональних даних, що може призвести, зокрема, до фізичних, матеріальних або нематеріальних збитків.

Аналіз ризиків надає числові значення для a) ймовірності та b) впливу/серйозності ризику. Множачи ці значення, можна визначити високий або низький рівень ризику.

2.2.4.1 Оцінка ймовірності

Необхідно здійснити оцінку ймовірності виникнення ризику, враховуючи, чи відбувався цей ризик раніше в організації або в подібній організації в тому ж економічному секторі чи географічному регіоні, а також чи є достатня мотивація, можливість і здатність для того, щоб загроза стала реальністю.

Ймовірність кожного ризику оцінюється в числових одиницях від 1 до 5. Загальні вказівки щодо оцінки числових одиниць наводяться в наступній таблиці. Оцінка ймовірності ризику повинна враховувати наявну інформацію та результати внутрішнього контролю. Залежно від об'єкта оцінки ризику, для кожного рівня ймовірності можуть використовуватися більш детальні вказівки.

Рівень	Заголовок	Опис
1	Малоймовірно	Це ніколи не відбувалося раніше, немає підстав вважати, що ймовірність збільшиться зараз
2	Неймовірно	Це може статися, але, ймовірно, не станеться
3	Ймовірно	Загалом ризик є більш ймовірним, ніж не ймовірним
4	Дуже ймовірно	Було б дивно, якби ризик не стався, враховуючи частоту в минулому та поточні обставини

5	Майже напевно	Або відбувається регулярно, або є підстави вважати, що ризик є невідворотним

2.2.4.2 Оцінка впливу/серйозності ризику

Необхідно провести оцінку впливу ризику на права та свободи суб'єктів даних та на організацію. При цьому слід враховувати наявні ефективні заходи контролю, які знижують вплив ризику.

Вплив слід оцінювати за наступними напрямами:

- Права та свободи суб'єктів даних (переважно клієнтів)
- Фінанси
- Охорона здоров'я та безпека
- Хороша репутація
- Юридичні, контрактні чи організаційні зобов'язання

Вплив кожного ризику слід оцінювати за числовою шкалою від 1 (низький) до 5 (високий). Наведена таблиця надає загальні вказівки для звітності всіх значень.

Залежно від обсягу оцінки ризику, можливо надати більш детальні вказівки для кожного рівня впливу.

Підстави для застосування певного рівня слід записувати, щоб полегшити інтерпретацію та забезпечити можливість повторюваності в майбутніх оцінках.

За необхідності, суб'єкти даних або їх представники повинні бути проконсультовані щодо передбачуваної обробки, без шкоди для захисту комерційних або публічних інтересів чи безпеки обробки.

Думки можуть бути отримані різними способами і, залежно від обставин (наприклад, загальне дослідження цілей та методів обробки, запит до представників керівництва чи стандартне опитування майбутніх клієнтів), необхідно забезпечити, щоб компанія мала належну правову основу для обробки даних, щодо яких запитуються думки.

Якщо остаточне рішення про обробку відрізняється від думки суб'єктів даних, необхідно задокументувати причини продовження або припинення обробки. Також слід документувати, якщо компанія не звертається до суб'єктів даних для отримання їх думки, оскільки вважає, що це не доцільно, наприклад, якщо це порушує конфіденційність бізнес-плану компанії або є непропорційним чи нереалістичним.

№	Опис	Права та свободи суб'єктів даних	Вплив на споживача	Фінансовий вплив	Здоров'я та безпека	Вплив на репутацію	Юридичний вплив
1	Незначний	Жодної дії, всі права і свободи гарантовані	Жодного впливу	Немає або дужу малий	Дуже невеликий додатковий ризик	Незначний	Жодного ефекту
2	Помірний	Невелике обмеження	Певні локальні збої в звичайних бізнес-операціях	Деякий	У прийнятній мірі	Низький	Невеликий ризик через нехтування зобов'язаннями
3	Поміркований	Помітне обмеження прав і свобод, але з метою обробки	Доставляти продукти/надавати послуги все ще можливо з деякими труднощами	Небажаний, але терпимо	Високий ризик; вимагає негайних дій	Поміркований	Реальна небезпека незаконних операцій
4	Високий	Невиправдане втручання в приватне життя	Серйозні втрати бізнесу в ключових областях	Серйозний вплив на дохід та/або прибуток	Значний ризик для життя	Високий	Незаконна діяльність у деяких областях
5	Дуже високий	Відповідальна особа зазнає шкоди	Економічний колапс	Нездатність функціонувати	Фактична або високоімовірна смерть	Дуже високий	Суворі штрафи, збитки та кримінальні наслідки

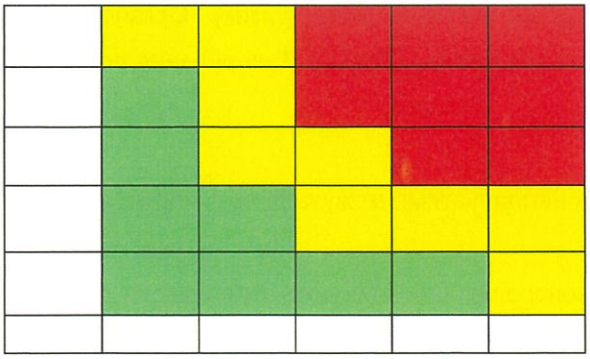
2.2.4.3 Класифікація ризику

На основі оцінки ймовірності та ступеня впливу/серйозності, для кожного ризику отримується значення шляхом множення двох чисел. Використовується матриця, показана на Рисунку 2, для визначення класифікації ризику на основі отриманого значення.

Усі ризики класифікуються відповідно до наступних значень, як показано в таблиці нижче.

ВИСОКИЙ - 5 або більше

НИЗЬКИЙ - 1-4



5	Високий	Високий	Високий	Високий	Високий
4	Низький	Високий	Високий	Високий	Високий
3	Низький	Високий	Високий	Високий	Високий
2	Низький	Низький	Високий	Високий	Високий
1	Низький	Низький	Низький	Низький	Низький
	1	2	3	4	5

2.2.5 Оцінка ризиків

Метою оцінки ризиків є визначення, які ризики є прийнятними, а які потребують управління. Матриця, позначена на попередньому малюнку, містить класифікацію ризиків. Зелений колір позначає ризик нижче допустимого рівня. Червоний колір зазвичай вказує на те, що ризик не відповідає критеріям прийняття ризику, і тому буде необхідне управління ризиками.

2.2.6 Визначення плану управління ризиками

Для тих ризиків, які були ідентифіковані вище як такі, що перевищують поріг компанії, необхідно розробити рішення для зменшення цих ризиків.

Загальна мета управління ризиками — зменшити рейтинг ризику до прийнятного рівня. Це не завжди можливо, оскільки іноді значення зменшується, але ризик залишається незмінним, наприклад, зниження з 8 до 6 все одно вказує на високий рівень ризику. Організація може вирішити прийняти ці ризики, незважаючи на високий рівень ризику. Такі рішення повинні бути задокументовані з відповідним поясненням.

2.2.6.1 Методи управління ризиками

Для управління ризиками, які були визначені як неприпустимі, можуть бути використані наступні методи:

- Модифікація ризику — застосування контролів, що знижують ймовірність і/або вплив ризику
- Уникнення ризику шляхом вжиття заходів, щоб забезпечити, що ризик більше не існує

- Спільне управління ризиком з іншими партнерами (наприклад, страховиком чи постачальником)

Рішення повинні ґрунтуватися на розгляді кроків, що повинні бути вжиті, і повинні базуватися на ґрунтовних знаннях обставин ризику. Зокрема:

- Бізнес-стратегія
- Регуляторні та юридичні міркування
- Технічні питання
- Комерційні та контрактні питання

2.2.6.2 Вибір контролів

Необхідно визначити відповідні контрелі для зниження ймовірності або впливу (або обох) усіх ризиків до прийнятних рівнів.

2.2.7 Звіт про оцінку ризиків/оцінку впливу

В результаті оцінки варіантів дій буде створено звіт про оцінку ризиків (та оцінку впливу на захист даних), який міститиме:

- Запропоновані операції з обробки та опис особистих даних
- Цілі обробки, включаючи, де це застосовно, законні інтереси контролера, визначені в GDPR
- Оцінка необхідності та пропорційності обробки
- Результат оцінки ризиків для прав і свобод суб'єктів даних
- Для кожного ризику, чи рекомендовано його прийняття чи обробка
- Черговість управління ризиками
- Менеджери ризиків
- Запропоновані варіанти управління ризиками
- Реалізація контролю/контролів
- Відповідальні за вжиті заходи
- Графік заходів
- Рівень залишкового ризику після реалізації контролів

Рекомендується використовувати програму на вебсайті НАЗК (DPIA) для документування звіту про оцінку впливу, але це не є обов'язковим.

2.2.8 Отримання погодження керівництва щодо залишкових ризиків

На всіх етапах оцінки впливу на захист даних керівництво повинно бути інформоване про хід роботи та прийняті рішення, включаючи офіційне прийняття залишкових ризиків, які передбачаються. Керівництво затверджує звіт про оцінку впливу та розглядає залишкові ризики, ухвалюючи рішення про подальші дії з огляду на ці ризики.

Остаточне погодження повинно бути позначене в спосіб, передбачений документами компанії.

2.2.9 Попереднє погодження з наглядовим органом

Якщо оцінка впливу на захист даних (DIA) вказує на високий ризик до реалізації запланованих заходів контролю, GDPR вимагає, щоб до початку обробки було проконсультовано наглядовий орган. Консультація повинна містити наступну інформацію:

- деталі відповідальності контролера, спільних контролерів та обробників, які залучені до обробки;
- цілі та методи запланованої обробки;
- застосовні заходи контролю за захистом даних;
- контактні дані посадової особи з питань захисту даних (якщо така є);
- копія звіту про оцінку впливу;
- інша інформація, яку може вимагати наглядовий орган.

Якщо орган нагляду виявить під час попередньої консультації, що вимоги, визначені чинним законодавством, не були повністю виконані стосовно передбаченої обробки, зокрема якщо буде вважати, що ризики, пов'язані з обробкою, не були належним чином ідентифіковані або пом'якшені контролером, він, окрім або замість інших заходів, що підпадають під його компетенцію, визначить необхідні кроки для усунення виявлених недоліків і запропонує контролеру або, в межах його діяльності, обробнику, заходи для їх реалізації.

Орган нагляду надасть свою пропозицію письмово протягом шести тижнів після початку попередньої консультації. Орган нагляду може продовжити цей термін максимум на один місяць, при цьому він повинен інформувати контролера або обробника про це та зазначити причини продовження протягом одного місяця з моменту початку попередньої консультації.

2.2.10 Застосування заходів управління ризиками

Після прийняття плану управління ризиками необхідні заходи повинні бути відстежені та реалізовані в рамках щоденного моніторингу проєкту. Якщо будь-які з заходів затримуються або не реалізуються, слід оцінити їхній вплив на захист персональних даних та ухвалити рішення щодо подальших дій. Якщо нерозв'язаний ризик є серйозним, це може мати значний вплив на здійсненність проєкту.

2.2.11 Моніторинг і звітування про ризики

За можливості ефективність контролів ризиків повинна бути виміряна та задокументована за допомогою об'єктивних показників.

2.2.12 Регулярний перегляд

Оцінка ризиків повинна переглядатися щорічно та регулярно, щоб забезпечити актуальність оцінок і правомірність застосованих заходів контролю. За необхідності має бути проведена позапланова оцінка ризиків, якщо зміни обставин це вимагають: наприклад, у разі значних змін у бізнесі, злиттів і поглинань, змін в IT-послугах/технологіях тощо.

2.2.13 Ролі та обов'язки

Учасники та їхні обов'язки в процедурах оцінки ризиків і контролю визначаються для кожного проєкту індивідуально відповідно до процесу, описаного вище. За потреби, до погодження керівництвом може бути залучений експерт з питань захисту даних.

2.3. РЕЄСТР УПРАВЛІННЯ ДАНИМИ

Усі контролери даних повинні вести Реєстр управління даними. Якщо контролер виступає як обробник даних у конкретній ситуації, Реєстр обробки даних повинен містити окремі дані про операції обробки. Форму Реєстру обробки даних наведено в Додатку 3 до цього Кодексу поведінки. За ведення реєстру відповідає Контактна точка з питань захисту даних (на момент видачі цього Кодексу — пані Анталь Сонтаг).

2.4. СИСТЕМА ЗАХИСТУ ДАНИХ КОНТРОЛЕРА

ЗАВДАННЯ ТА ОБОВ'ЯЗКИ ОРГАНІЗАЦІЙНИХ АКТОРІВ

2.4.1. КОНТРОЛЕР ДАНИХ

EWG Customs Agency Services Private Limited Company є контролером даних для обробки даних, що покриваються цією Політикою.

Дані, що стосуються Контролера даних:

- Назва: EWG Customs Agency Services Private Limited Company
- Скорочена назва: EWG Customs Agency Ltd.
- Реєстраційний номер компанії: 01-10-141551
- Податковий номер: 27438635-2-41
- Адреса: 1134 Budapest, Róbert Károly körút 59.
- Електронна пошта: info@ewgcustoms.com
- Номер телефону: +36 1/866-3070

2.4.2. ОФІЦЕР ЗАХИСТУ ДАНИХ (DPO)

Контролер і обробник повинні призначити офіцера з захисту даних у таких випадках:

- коли обробка здійснюється органами державної влади або іншими установами, що виконують публічні обов'язки, за винятком судів, які діють у межах своїх юрисдикційних повноважень;
- коли основна діяльність контролера чи обробника включає систематичну і великомасштабну моніторинг даних суб'єктів даних, за своєю природою, масштабом та/або цілями;

- коли основна діяльність контролера чи обробника включає обробку великої кількості даних, що стосуються спеціальних категорій персональних даних згідно зі статтею 9 GDPR і рішень щодо кримінальної відповідальності та злочинів, зазначених у статті 10.

Офіцер з захисту даних повинен бути призначений на основі професійної компетентності, зокрема експертних знань у сфері захисту даних та здатності виконувати обов'язки офіцера з захисту даних.

Офіцер з захисту даних може бути працівником контролера або обробника, або зовнішнім постачальником послуг за договором про надання послуг. У разі призначення працівника компанії необхідно забезпечити, щоб працівник, призначений офіцером з захисту даних, не брав участі в жодному етапі обробки (незалежність), тобто він не може бути особою, яка визначає мету, обсяг або необхідність обробки. Офіцер з захисту даних також може виконувати інші завдання. Контролер або обробник повинні забезпечити, щоб ці завдання не призводили до конфлікту інтересів.

2.4.3. Процедура прийняття рішення щодо призначення офіцера з захисту даних

Необхідно задокументувати внутрішній аналіз, щоб визначити, чи потрібно компанії призначити офіцера з захисту даних, для того щоб продемонструвати, що всі відповідні фактори були належним чином оцінені під час прийняття рішення, якщо тільки не очевидно, що організація не зобов'язана призначати офіцера з захисту даних. Як і з усіма питаннями, пов'язаними з конфіденційністю, ця документація повинна оновлюватися, наприклад, коли з'являються нові види діяльності або послуги, що потрапляють під обов'язкові вимоги щодо призначення офіцера з захисту даних.

Компанія не є органом державної влади або іншою установою з публічними обов'язками, тому стаття 37(1)(a) GDPR не застосовується. Основна діяльність компанії не включає обробку великої кількості даних, що стосуються спеціальних категорій персональних даних відповідно до статті 9 GDPR та рішень щодо кримінальної відповідальності та злочинів, зазначених у статті 10 GDPR, і тому стаття 37(1)(c) GDPR до неї не застосовується.

Основна діяльність компанії полягає в наданні інших послуг, допоміжних до транспорту. Компанія обробляє лише обмежену кількість персональних даних і лише у зв'язку з її основною діяльністю. Враховуючи ці факти та вищезазначені обов'язкові положення, керівництво компанії вважає, що компанія не підпадає під обов'язкові вимоги і тому було прийнято рішення не призначати офіцера з захисту даних.

2.5. ОБОВ'ЯЗОК КОНТРОЛЕРА НАДАТИ ІНФОРМАЦІЮ

Контролер даних зобов'язаний надати суб'єкту даних інформацію про обробку його або її персональних даних в стислій, прозорій, зрозумілій та легкодоступній формі, простими та зрозумілими словами.

2.5.1. Процедурні правила

Існують два основних способи отримання персональних даних, як зазначено в GDPR:

a) збір персональних даних від самого суб'єкта даних (Стаття 13 GDPR)

b) отримання персональних даних не від суб'єкта даних (Стаття 14 GDPR)

У обох випадках GDPR перераховує інформацію, яку потрібно надати суб'єкту даних. Крім того, можна надати додаткову інформацію. Під час складання цього Повідомлення слід врахувати такі питання:

2.5.1.1 Чи має суб'єкт даних вже цю інформацію?

GDPR вимагає, щоб суб'єкти даних були поінформовані про зазначену інформацію, якщо вони ще не отримали її. Тому важливо встановити, чи має суб'єкт даних всю необхідну інформацію, яку слід надати, і чи можна це належним чином перевірити.

Якщо це так, попередню інформацію слід задокументувати та зберігати як доказ дотримання GDPR. Виникнення та перевірка цієї інформації повинні оцінюватися індивідуально для кожного суб'єкта даних.

2.5.1.2 Якщо персональні дані збираються безпосередньо від суб'єкта даних

У випадках, коли суб'єкт даних не має необхідної інформації (наприклад, коли дані збираються на вебсайті безпосередньо від користувачів або працівників), необхідно надати наступну інформацію під час збору персональних даних:

- ідентифікація та контактні дані контролера та, за потреби, представника контролера;
- цілі, для яких персональні дані обробляються, та правова основа для обробки;
- законні інтереси контролера або третьої сторони;
- як обробляються дані;
- за потреби, одержувачі персональних даних та категорії одержувачів, якщо такі є;
- за потреби, факт та деталі наміру контролера передати персональні дані до третьої країни або міжнародної організації;
- тривалість зберігання персональних даних або, якщо це неможливо, критерії для визначення цієї тривалості;
- інформація про права суб'єкта даних на запит до контролера щодо доступу, виправлення або видалення персональних даних, що стосуються його чи її, а також право на перенесення даних;
- інформація про права суб'єкта даних на запит до контролера обмежити обробку персональних даних щодо нього або її та заперечувати проти обробки таких персональних даних;
- інформація про право суб'єкта даних відкликати свою згоду в будь-який час;
- інформація про право суб'єкта даних подати скаргу до наглядового органу;
- чи є надання персональних даних юридичним або контрактним зобов'язанням та можливі наслідки непредставлення даних;

– чи здійснюється автоматизоване прийняття рішень, включаючи профілювання, і принаймні в таких випадках — логіка, що використовується.

2.5.1.3 Якщо персональні дані не були отримані від суб'єкта даних

Якщо персональні дані не були отримані від суб'єкта даних (наприклад, коли дані надаються компанії третьою стороною), існує кілька інших обставин (тобто, не рахуючи випадку, коли суб'єкт даних вже має цю інформацію), коли інформація не повинна надаватися. Це включає:

– якщо надання цієї інформації є неможливим або вимагає непропорційних зусиль;
– якщо отримання або розголошення даних прямо передбачено законодавством ЄС або держави-члена, що застосовується до контролера, яке забезпечує належні заходи для захисту законних інтересів суб'єкта даних (Стаття 14 GDPR);
– якщо персональні дані повинні залишатися конфіденційними згідно з обов'язком професійної таємниці, накладеним законодавством ЄС або держави-члена.

Коли будь-яка з цих умов застосовується, причина цього повинна бути належним чином задокументована та збережена як доказ дотримання GDPR. Слід забезпечити, щоб це застосовувалося до всієї необхідної інформації та всіх суб'єктів даних.

2.5.3. Інформація для суб'єкта даних

Якщо жодна з наведених вище умов не виконана, суб'єкти даних повинні бути поінформовані:

– протягом розумного часу з моменту отримання персональних даних, але не пізніше одного місяця;
– якщо персональні дані використовуються для контакту з суб'єктом даних (наприклад, електронні адреси), то принаймні на момент першого контакту з суб'єктом даних;
– якщо дані ймовірно будуть передані іншим отримувачам, не пізніше, ніж коли персональні дані будуть вперше передані.

Наступна інформація повинна бути надана:

– ідентифікація та контактні дані контролера та, якщо є, представника контролера;
– контактні дані посадової особи з питань захисту даних (DPO), якщо така є;
– цілі, для яких персональні дані будуть оброблятися, та правова основа для обробки;
– категорії персональних даних, що стосуються обробки;
– отримувачі персональних даних або категорії отримувачів, якщо такі є;
– за потреби, факт та деталі наміру контролера передати персональні дані до третьої країни чи міжнародної організації;
– тривалість зберігання персональних даних або, якщо це неможливо, критерії для визначення цієї тривалості;
– інформація про права суб'єкта даних на запит до контролера щодо доступу до, виправлення або видалення персональних даних, що стосуються його або її, а також право на перенесення даних;

- інформація про права суб'єкта даних на запит до контролера обмежити обробку персональних даних щодо нього або неї та заперечувати проти обробки таких персональних даних;
- інформація про право суб'єкта даних відкликати свою згоду в будь-який час;
- інформація про право суб'єкта даних подати скаргу до наглядового органу;
- джерело персональних даних;
- чи здійснюється автоматизоване прийняття рішень, включаючи профілювання, і, принаймні в таких випадках, логіка, що використовується.

2.5.4. Способи надання інформації суб'єкту даних

Як і всю інформацію, надану суб'єктам даних у рамках GDPR, вона повинна бути надана в ясній та доступній формі, простими і зрозумілими словами. Кращий спосіб надання інформації залежатиме від специфіки бізнес-процесу та може включати наступне:

- Сповіщення на вебсайті
- Через електронну пошту
- Через друковані листи/брошури
- По телефону

Якщо персональні дані будуть використані для іншої мети, ніж та, для якої вони були зібрані, інформація повинна бути надана суб'єкту даних знову, відповідно до нової мети, до початку обробки для цієї іншої мети.

Факт надання інформації повинен бути належним чином задокументований для підтвердження. Це означає, що (i) якщо інформація надається через вебсайт, необхідно перевірити, що суб'єкт даних має доступ до повної інформації та активно приймає її (відмічає галочку або натискає кнопку "прийняти" тощо), (ii) якщо інформація надається електронною поштою, необхідно підтвердити отримання листа, (iii) якщо через лист, підтвердження отримання має бути надане, (iv) якщо особисто, підтвердження отримання повинно бути надано, а (v) телефонний дзвінок має бути належним чином зафіксований.

У межах організації особа, яка призначена для затвердження змісту інформаційних листів, — це генеральний директор.

2.6. ОБРОБКА ЗАПИТІВ ВІД СУБ'ЄКТІВ ДАНИХ

Згідно з GDPR, суб'єкти даних мають широкі права щодо своїх даних, і важливо, щоб організація була готова забезпечити дотримання цих прав та виконувати запити вчасно.

2.6.1 Загальні правила

Кожен запит від суб'єкта даних підлягає наступним загальним правилам:

- Інформація повинна бути надана суб'єкту даних у стислій, прозорій, зрозумілій та легкодоступній формі, ясною та простою мовою, зокрема для інформації, що надається дітям;

- Інформація повинна надаватися письмово або іншими засобами, включаючи електронні засоби, за потреби;
- За запитом суб'єкта даних також може бути надана усна інформація (наприклад, телефоном або особисто), за умови, що особа суб'єкта даних була належним чином ідентифікована;
- Ми не можемо відмовити у виконанні запиту суб'єкта даних на реалізацію його прав, якщо не можемо довести, що ми не можемо ідентифікувати суб'єкта даних;
- Без зайвих затримок, але не пізніше одного місяця з моменту отримання запиту, ми повинні повідомити суб'єкта даних про вжиті заходи стосовно запиту; за необхідності, з урахуванням складності запиту та кількості запитів, цей строк може бути подовжений на два місяці. Подовження терміну повинно бути повідомлено суб'єкту даних протягом одного місяця з моменту отримання запиту та має містити причини затримки;
- Якщо запит був поданий електронними засобами, інформація повинна бути надана також електронними засобами, якщо це можливо, якщо тільки суб'єкт даних не запитає інше;
- Якщо ми не вживаємо заходів щодо запиту суб'єкта даних, ми повинні негайно, але не пізніше одного місяця з моменту отримання запиту, повідомити суб'єкта даних про причини відмови та право подати скаргу до наглядового органу та звернутися до суду;
- Інформація та дії повинні надаватися безкоштовно, якщо тільки запит суб'єкта даних не є «очевидно безпідставним або надмірним, зокрема через його повторюваний характер» (Стаття 12 GDPR). У таких випадках ми можемо стягувати адміністративний збір за витрати або відмовитися виконувати запит; адміністративний збір розраховується таким чином: a) якщо запит не потребує надання носія інформації або фотокопіювання паперової документації, збір складає 3000 HUF за годину; b) якщо дані надаються на носії інформації, додається вартість носія та збір за пункт (a); c) якщо необхідне фотокопіювання паперових документів, стягується додатково 100 HUF за сторінку;
- Якщо у нас є обґрунтовані сумніви щодо ідентичності фізичної особи, ми можемо запросити додаткову інформацію, необхідну для підтвердження ідентичності суб'єкта даних.

2.6.2 Кроки процедури

Крок	Опис	Відповідальний
Отримання запиту суб'єкта даних	Запит може бути поданий суб'єктом даних електронно (електронною поштою або через наш вебсайт), поштою або телефоном. Він може бути прийнятий будь-якою частиною організації, але бажано, щоб запит надходив через службу підтримки.	Адміністратор прийому/отримання

Реєстрація запитів суб'єктів даних	Факт і дата отримання запиту повинні бути зафіксовані в Реєстрі запитів суб'єктів даних. У реєстрі мають бути зазначені дані особи, що подала запит (ім'я, адреса, інші ідентифікаційні дані), тип запиту (видалення, виправлення, зміна даних тощо), що саме з даних стосується запит, та причини запиту. Якщо запит неясний, це має бути повідомлено суб'єкту даних без затримок разом із уточненням змісту запиту.	Адміністратор запитів
Перевірка особи	Ідентичність особи перевіряється згідно з внутрішньою процедурою, залежно від способу подання запиту. За потреби може бути запитана додаткова інформація для підтвердження ідентичності. Якщо суб'єкт даних не зможе підтвердити свою ідентичність, запит буде відхилено, і причини цього будуть повідомлені суб'єкту даних без затримки, але не пізніше ніж через один місяць після отримання запиту.	Адміністратор запитів
Оцінка правомірності запиту	Потрібно провести перевірку, чи є запит "очевидно безпідставним або надмірним". Це можна зробити, перевіривши Реєстр запитів суб'єктів даних на наявність схожих запитів від того самого суб'єкта та оцінити тип запиту. Якщо запит схожий на попередній, буде прийнято рішення про відмову або нарахування додаткової плати. У разі запиту на виправлення, видалення, обмеження обробки або заперечення проти обробки, слід прийняти рішення про його доцільність та правомірність. Якщо запит не правомірний, він буде відхилений. Суб'єкту даних слід повідомити про відмову, а також про право подати скаргу до наглядового органу і звернутися до суду.	Адміністратор запитів
Нарахування плати	Якщо нараховується плата, особа має бути повідомлена про це та отримати можливість прийняти рішення щодо подальших дій. Якщо особа вирішить не продовжувати, запит буде відхилено, і причини цього будуть повідомлені без затримки.	Адміністратор запитів

Збір запитуваної інформації	Якщо запит є правомірним і може бути виконаний, необхідно зібрати відповідну інформацію відповідно до типу запиту. Це включатиме планування того, як буде виконано запитану операцію (наприклад, обмеження або видалення обробки даних). Запит має бути виконаний протягом максимум одного місяця, що може бути продовжено ще на два місяці. Про продовження терміну потрібно повідомити суб'єкта даних протягом одного місяця з моменту отримання запиту, зазначивши причини затримки.	Адміністратор запитів / Власник даних
Виконання запиту/надання запитуваної інформації	Запитану операцію потрібно виконати (якщо це можливо), а запитувану інформацію надіслати суб'єкту даних електронними засобами, якщо він цього бажає, або письмово поштою.	Адміністратор запитів
Закриття запиту суб'єкта даних	Факт і спосіб відповіді на запит (виконання/відмова) повинні бути зафіксовані в Реєстрі запитів суб'єктів даних разом із датою закриття запиту.	Адміністратор запитів

2.6.3 Можливі запити суб'єкта даних

2.6.3.1 Право на відкликання згоди

Коли правовою підставою для обробки є згода суб'єкта даних (і немає іншої правової підстави, такої як виконання договору або юридичного зобов'язання), суб'єкт даних має право відкликати свою згоду.

Перед видаленням особистих даних суб'єкта з обробки необхідно підтвердити, що згода є дійсною правовою підставою для обробки. Якщо ні, запит може бути відхилений через те, що обробка ґрунтується на іншій правовій підставі, і згода суб'єкта даних не є необхідною. В іншому випадку запит має бути виконаний. Всі запити повинні бути оцінені детально, і виконані в максимально можливому обсязі, з наданням причин для будь-якої відмови (включаючи часткові відмови).

Контролер повинен забезпечити, щоб суб'єкт даних міг відкликати свою згоду в будь-який час, і повинен дозволити відкликання згоди таким самим простим способом, як і надання згоди. У більшості випадків можна дати і відкликати згоду електронно, тобто онлайн (наприклад, видаливши свій профіль), тому ця процедура зазвичай не є необхідною.

Якщо згода дитини є необхідною (осіб до 16 років), особа, яка має батьківську опіку над дитиною, повинна схвалити надання або відкликання згоди, і ідентичність цієї особи також повинна бути перевірена та зафіксована в Реєстрі запитів суб'єктів даних у розділі "Примітки".

2.6.3.2 Право на інформацію

Під час отримання особистих даних суб'єкта, цей суб'єкт має бути проінформований про факт обробки, мету, правову підставу, обсяг оброблюваних даних, метод, тривалість або критерії визначення тривалості обробки, правила щодо портативності даних, а також право подати скаргу до наглядового органу.

Окрім цієї інформації, суб'єкт даних повинен бути чітко проінформований про можливість здійснення права на заперечення, і ця інформація має бути чітко виділена окремо від іншої інформації.

Інформація:

(a) надається заявникам на сторінці, де публікується оголошення про вакансію, відповідно до відповідного повідомлення про обробку даних;

(b) особам, які встановлюють трудові чи інші трудові відносини з Контролером даних, під час встановлення правовідносин, з відповідним змістом повідомлення про обробку даних;

(c) надається особам, які входять на територію Контролера, до входу на територію, відповідно до змісту відповідного повідомлення про конфіденційність.

Інформація, зазначена в пункті (a), повинна бути доступна на вебсайті Контролера даних у стислому, прозорому та легкодоступному вигляді, зрозумілою та простим мовою. Інформація, зазначена в пункті (b), повинна надаватися в електронному вигляді під час встановлення правовідносин, а особа повинна надати письмове підтвердження цього у вигляді паперової заяви.

Інформація, зазначена в пункті (c), повинна бути розміщена за допомогою оголошення або вивіски на огорожі або вхідних воротах на межі території.

2.6.3.3 Право доступу суб'єкта даних

Суб'єкти даних мають право отримати від нас інформацію щодо того, чи обробляються їх особисті дані, і якщо так, то вони мають право на доступ до своїх особистих даних та наступної інформації:

- мета обробки;
- категорії особистих даних, що обробляються;
- отримувачі або категорії отримувачів, яким або з якими ми розкрили або будемо розкривати особисті дані, зокрема отримувачі в третіх країнах або міжнародних організаціях;
- передбачуваний період зберігання особистих даних або, якщо це неможливо, критерії визначення цього періоду;
- право суб'єкта даних отримати від нас виправлення, видалення або обмеження обробки особистих даних, що стосуються його, а також право на заперечення проти обробки таких особистих даних;
- право подати скаргу до наглядового органу;
- якщо дані не були зібрані у суб'єкта даних, будь-яка доступна інформація про їх джерело;

– факт автоматизованого прийняття рішень, включаючи профілювання, та інформація про ймовірні наслідки для суб'єкта даних;

– якщо особисті дані передаються до третьої країни або міжнародної організації, суб'єкт даних має право бути поінформованим про відповідні заходи захисту при передачі.

Доступ до персональних даних має бути забезпечений таким чином, щоб суб'єкт даних, наскільки це можливо, не зміг дізнатися про персональні дані іншої особи. Виняток може бути зроблений для персональних даних, які стосуються як суб'єкта даних, так і іншої особи.

Контролер даних може обмежити або відмовити в праві доступу суб'єкта даних пропорційно до мети, яку переслідує це обмеження, коли така міра є строго необхідною:

a) для ефективного і результативного проведення розслідувань чи процедур, що стосуються контролера даних, зокрема кримінальних справ;

b) для ефективного і результативного запобігання та виявлення кримінальних правопорушень;

c) для виконання покарань і заходів проти правопорушників;

d) для ефективного і результативного захисту публічної безпеки;

e) для ефективного і результативного захисту зовнішньої та внутрішньої безпеки держави, зокрема національної оборони та національної безпеки;

f) для забезпечення захисту основних прав третіх осіб.

Якщо контролер даних відмовляє або обмежує право доступу суб'єкта даних, він негайно інформує суб'єкта даних письмово, вказуючи причини такої міри, якщо це не загрожує меті обмеження або відмови. У повідомленні контролер особливо звертає увагу суб'єкта даних на те, що він може скористатися правом доступу за допомогою наглядового органу. Якщо оброблювані дані зберігаються або резервуються у вигляді аудіо- чи відеозаписів, матеріал надається у оригінальній формі, а транскрипти чи витяги будуть достатніми лише у разі знищення оригінальних записів.

2.6.3.4 Право на виправлення

На запит суб'єкта даних відповідальний адміністратор обробки даних має виправити неточні персональні дані, що стосуються суб'єкта даних, без необґрунтованої затримки. З урахуванням мети обробки, суб'єкт даних також має право вимагати доповнення неповних персональних даних, зокрема за допомогою додаткової заяви.

У разі необхідності компанія вживає заходів для перевірки інформації від суб'єкта даних, щоб забезпечити її точність перед записом (наприклад, консультуванням з особистими документами).

2.6.3.5 Право на стирання ("право на забуття")

На запит суб'єкта даних контролер або DPO має без необґрунтованої затримки видалити персональні дані суб'єкта даних або набір персональних даних, зазначених суб'єктом даних, якщо має місце одна з таких ситуацій:

– персональні дані більше не необхідні для цілей, для яких вони були зібрані або іншим чином оброблялись;

– суб'єкт даних відкликає згоду, на підставі якої проводиться обробка, і немає іншої правової підстави для обробки;

– суб'єкт даних заперечує проти обробки на підставі статті 21(1) GDPR, і немає переважних законних підстав для обробки, або суб'єкт даних заперечує проти обробки на підставі статті 21(2) GDPR;

– персональні дані оброблялись незаконно;

– персональні дані повинні бути видалені для виконання юридичних зобов'язань відповідно до законодавства ЄС або національного законодавства.

Розумні зусилля повинні бути докладені для забезпечення видалення даних, якщо ці дані були розкриті. Це означає, що, з урахуванням наявних технологій та витрат на їх використання, компанія повинна вжити всіх розумних заходів для інформування контролера персональних даних про те, що суб'єкт даних запитав у контролера видалення посилань на такі персональні дані, а також їх копій і реплік.

Контролер не може видаляти персональні дані, незважаючи на обґрунтований запит, якщо обробка необхідна:

- для здійснення права на свободу вираження поглядів та інформації;
- для виконання юридичного зобов'язання;
- в інтересах громадськості в галузі охорони здоров'я;
- для архівування в інтересах суспільства, наукових або історичних досліджень чи статистичних цілей;
- для встановлення, здійснення або захисту юридичних вимог.

Ймовірно, що ці рішення потребуватимуть залучення Офіцера з захисту даних компанії, якщо такий є, а в деяких випадках і вищого керівництва компанії.

2.6.3.6 Право на обмеження обробки

На запит суб'єкта даних відповідальний адміністратор, що здійснює обробку, повинен обмежити обробку, якщо виконано одну з таких умов:

- суб'єкт даних оскаржує точність персональних даних, у такому випадку обмеження застосовується на період, що дозволяє перевірити точність персональних даних;
- обробка даних є незаконною, і суб'єкт даних проти їх видалення, вимагаючи натомість обмеження їх використання;
- контролер більше не потребує персональних даних для цілей обробки, але суб'єкт даних потребує їх для встановлення, здійснення або захисту юридичних вимог;
- суб'єкт даних заперечує проти обробки; у цьому випадку обмеження застосовується до з'ясування, чи переважають законні підстави контролера над підставами суб'єкта даних.

Суб'єкт даних, який обмежив обробку, повинен бути поінформований до того, як обмеження буде зняте.

Для кожного такого запиту компанія повинна прийняти рішення щодо того, чи задовольняти запит. Ймовірно, що ці рішення потребуватимуть залучення Офіцера з захисту даних компанії, якщо такий є, а в деяких випадках і вищого керівництва компанії.

Коли обробка обмежується, як зазначено вище, такі персональні дані, за винятком зберігання, можуть оброблятися лише за згодою суб'єкта даних або для встановлення, здійснення або захисту юридичних вимог чи для захисту прав іншої фізичної або юридичної особи, або для важливих публічних інтересів Союзу або держави-члена.

(3) Адміністратор, що здійснює обробку, повинен повідомити суб'єкта даних, у запиті якого було обмежено обробку, про зняття обмеження обробки заздалегідь.

Обов'язок інформувати отримувачів і оброблювачів

Контролер персональних даних повинен поінформувати всіх отримувачів та оброблювачів, яким він передав або з якими він комунікував персональні дані, про будь-яку виправлення, видалення або обмеження обробки персональних даних, якщо це не є неможливим або не вимагає непропорційних зусиль.

2.6.3.7 Право на переносимість даних

На запит суб'єкта даних, відповідальний адміністратор, що здійснює обробку, повинен забезпечити переносимість персональних даних, за умови, що виконуються такі умови:

a) персональні дані були надані контролеру суб'єктом даних;

b) правова підстава для обробки – це згода або контракт між суб'єктом даних і контролером;

c) обробка здійснюється автоматизованими засобами;

d) обробка персональних даних не порушує права або свободи інших осіб.

При здійсненні права на переносимість даних, контролер персональних даних повинен надати персональні дані суб'єкту даних у структурованому, загальновживаному, машинозчитуваному форматі (PDF/XML).

Суб'єкт даних може попросити контролера передати персональні дані безпосередньо іншому контролеру. Суб'єкт даних може скористатися цією опцією лише в разі, якщо це технічно можливо. Контролер персональних даних також зобов'язаний надавати персональні дані на папері для полегшення здійснення права на доступ.

Послуги в цій категорії вимагають мінімального процесу ухвалення рішення для кожного випадку, і дуже бажано, щоб цей процес був автоматизований.

2.6.3.8 Право на заперечення

Суб'єкт даних має право на заперечення в будь-який час, з огляду на свою конкретну ситуацію, проти обробки своїх персональних даних на таких правових підставах:

- обробка необхідна для виконання завдання, що здійснюється в інтересах громадськості або в рамках використання офіційної влади, наданої контролеру;
- обробка необхідна для цілей законних інтересів, переслідуваних контролером або третєю стороною, за винятком випадків, коли ці інтереси переважаються інтересами або

основними правами та свободами суб'єкта даних, які вимагають захисту персональних даних, зокрема коли суб'єктом даних є дитина.

2.6.3.9 Автоматизоване прийняття рішень у індивідуальних випадках, включаючи профілювання

Суб'єкт даних має право не піддаватися рішенню, яке базується виключно на автоматизованій обробці, включаючи профілювання, яке має юридичні наслідки для нього або її, або подібним чином значно впливає на нього або її, а також має право на обґрунтовану людську участь, де це необхідно. Суб'єкт даних має право висловлювати свою думку і оскаржувати рішення.

Існують певні винятки з цього права, які застосовуються, якщо рішення:

- необхідне для укладення або виконання контракту;
- дозволено законом;
- ґрунтується на явній згоді суб'єкта даних.

При оцінці цього типу запиту необхідно визначити, чи застосовуються вказані вище винятки в конкретному випадку.

2.6.3.10 Право на відшкодування шкоди

У разі порушення своїх прав щодо обробки даних, суб'єкт даних може звернутися до служби підтримки контролера даних за адресою adatvedelem@ewgcustoms.com, яка розгляне скаргу та, якщо вона буде обґрунтованою, ініціює дії з генеральним директором контролера даних, інакше скарга буде відхилена.

Контролер даних повинен письмово поінформувати заявника про відмову впродовж 30 днів з моменту отримання запиту, зазначивши фактичні та юридичні підстави для відмови. У разі відмови у задоволенні запиту заявник також має бути проінформований про можливість звернення до суду та до наглядового органу. Адміністратор контролера зберігає запис про відхилені заяви.

Якщо суб'єкт даних має претензії щодо того, як контролер обробляє його або її дані, або якщо він або вона хоче звернутися до органу безпосередньо, він або вона може подати скаргу до Національного органу з захисту даних та свободи інформації (адреса: 1055 Будапешт, вулиця Фалк Мікша 9-11, поштове відправлення: 1363 Будапешт, поштове відділення 9, електронна пошта: ugyfelszolgalat@naih.hu, вебсайт: www.naih.hu).

Суб'єкт даних також має право звернутися до суду для захисту своїх персональних даних, який прийме рішення позачергово. У такому випадку суб'єкт даних може вибрати, чи подавати позов до суду за місцем проживання (постійною адресою) або місцем перебування (тимчасовою адресою) (http://birosag.hu/torvenyszekek).

Суб'єкт даних може звертатися до суду за місцем проживання або перебування за допомогою ресурсу: http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso.

2.7. ПРАВИЛА УПРАВЛІННЯ ДОКУМЕНТАМИ І ЇХ УТИЛІЗАЦІЇ

Правила управління документами та їх утилізації, що діють у Компанії, викладені в чинних правилах управління документами та їх утилізації.

2.8. ВИМОГИ ДО БЕЗПЕКИ ДАНИХ

Контролер зобов'язаний впроваджувати відповідні технічні та організаційні заходи для забезпечення та демонстрації того, що обробка персональних даних здійснюється відповідно до вимог GDPR, враховуючи характер, обсяг, контекст та цілі обробки, а також різні ступені ймовірності та серйозності ризику для прав і свобод фізичних осіб. Включаючи, коли це застосовно:

a) псевдонімізацію та шифрування персональних даних;

b) постійну конфіденційність, цілісність, доступність та стійкість систем та послуг, що використовуються для обробки персональних даних;

c) у разі фізичного або технічного інциденту — здатність відновити доступ до персональних даних і їх доступність у своєчасний спосіб;

d) процедуру регулярного тестування, оцінки та перевірки ефективності впроваджених технічних і організаційних заходів для забезпечення безпеки обробки.

При визначенні відповідного рівня безпеки необхідно чітко враховувати ризики, що виникають внаслідок обробки, зокрема випадкове або незаконне знищення, втрату, зміну, несанкціоноване розкриття або доступ до персональних даних, що передаються, зберігаються або іншим чином обробляються.

Контролер має впроваджувати відповідні технічні та організаційні заходи для забезпечення ефективної реалізації принципів, викладених у цій Політиці, та інтеграції додаткових заходів захисту даних в процес обробки даних.

Контролер також зобов'язаний впроваджувати відповідні технічні та організаційні заходи для забезпечення того, щоб за замовчуванням оброблялися лише ті персональні дані, які необхідні для конкретної мети обробки. Це зобов'язання стосується обсягу зібраних персональних даних, міри їх обробки, терміну зберігання та доступності. Ці заходи повинні, зокрема, гарантувати, що персональні дані не можуть за замовчуванням бути доступні невизначеній кількості осіб без втручання фізичної особи.

Документи, що містять персональні дані, не повинні залишатися в місцях, де до них може мати доступ стороння особа. Такі документи повинні бути зачинені в офісах або кімнатах персоналу, де можуть перебувати сторонні особи, окрім уповноважених осіб, які займаються обробкою документів.
Для запобігання втраті персональних даних, що обробляються вручну, оригінали документів повинні видаватися лише у ході офіційних справ, зокрема судових розглядів або слідчих процедур. Перед видачею має бути зроблена повна копія оригінальних документів для зберігання в компетентному підрозділі.

У разі пошкодження або знищення персональних даних повинні бути вжиті заходи для відновлення пошкоджених даних з доступних джерел даних. Керівник підрозділу, де сталося пошкодження, несе відповідальність за відновлення пошкоджених даних. До процесу відновлення даних має бути залучено компетентного контролера даних, який брав участь в їх реєстрації. Факт відновлення даних має бути зафіксований на замінених даних.

Персональні дані, що обробляються компанією, зберігаються компанією в електронній та/або паперовій формі.

Компанія використовує відповідні організаційні та технічні заходи для забезпечення безпеки даних. При визначенні відповідного рівня безпеки ми чітко враховуємо ризики, що виникають внаслідок обробки персональних даних, зокрема ризики, що пов'язані з випадковим або незаконним знищенням, втратою, зміною, несанкціонованим розкриттям або доступом до персональних даних, що передаються, зберігаються чи іншим чином обробляються.

Дані, що зберігаються в електронній формі, зберігаються на спеціалізованому сервері в головному офісі або філії компанії.

Електронна пошта хоститься за допомогою O365, послуги, наданої Microsoft як обробником даних.

Резервні копії на локальному обладнанні регулюються політикою IT.

Додаткові організаційні та IT-заходи для забезпечення безпеки електронно збережених даних викладені в IT-політиці.

Паперові документи, що містять персональні дані, зберігаються відповідно до специфічних правил архівування. Папки, що містять персональні дані, зберігаються в замкненій шафі в головному офісі компанії, яку відкривають та закривають щодня. Ключі від шафи зберігаються в

замкненому сейфі. Доступ до шаф для архівування визначається бізнес-підрозділом згідно зі специфічними інструкціями.

Заходи безпеки для доступу до філії викладені в Політиці безпеки об'єкта.

Контролер даних має забезпечити виконання вимог безпеки даних шляхом цих правил та окремих інструкцій і регламентів. Контролер даних має забезпечити, щоб його співробітники та треті особи, які діють від його імені (особливо обробники даних), були ознайомлені з вмістом цієї Політики та окремих інструкцій і регламентів, що діють у будь-який час, і діяли відповідно до них.

2.9. КОНКРЕТНІ ВИПАДКИ ОБРОБКИ ДАНИХ

2.9.1. Обробка даних співробітників

Контролер даних зобов'язаний інформувати всіх співробітників або інших осіб, які укладають трудовий договір, про обробку даних, пов'язаних з їх трудовою діяльністю. Особа, чиї дані обробляються, повинна письмово підтвердити, що вона була поінформована.

Дані, що містяться у реєстрах заробітної плати та трудових відносин, можуть бути використані для встановлення фактів, що стосуються правового статусу працівника, для перевірки вимог щодо класифікації, для обробки заробітної плати, соціального забезпечення та статистичного звітування.

В міру необхідності для виконання своїх обов'язків, реєстри заробітної плати та трудових відносин повинні бути під управлінням відповідального працівника Контролера даних, який займається кадровими питаннями.

2.9.2. Ручна обробка персональних даних

Контролер даних має враховувати сучасний рівень технологій при визначенні та впровадженні заходів для забезпечення безпеки даних. Необхідно вибрати з кількох можливих рішень обробки таке, яке забезпечує вищий рівень захисту персональних даних, якщо це не накладає непропорційну тягар на компанію.

Для забезпечення безпеки ручної обробки персональних даних необхідно вжити наступних заходів: a) Документи, що зберігаються в архівах, повинні зберігатися в замкненій, сухій кімнаті, обладнаній засобами протипожежного захисту та охорони майна; b) Доступ до документів, що перебувають у постійному активному управлінні, мають лише компетентні адміністратори, а кадрові, трудові та заробітні документи повинні зберігатися в надійно закритому вигляді; c) Архівування записів обробки даних повинно проводитися регулярно, і архівовані записи повинні сортуватися та зберігатися відповідно до відповідних вимог.

Правила доступу до ключів від кімнат чи шаф, зазначених у пункті (b), повинні бути визначені Генеральним директором Контролера даних.

2.9.3. Персональні дані, що обробляються електронно

Якщо Контролер даних обробляє персональні дані в електронній системі, доступ до якої має лише зареєстрований, компетентний працівник, що входить до списку доступу, такий працівник повинен увійти в систему за допомогою індивідуального, секретного пароля. Після завершення обробки працівник повинен вийти з системи. Контролер даних несе відповідальність за обробку даних, захищених паролем, у системі.

Для уникнення порушень даних відповідальність за захист індивідуального пароля покладається на працівника. Окрім працівника, індивідуальний пароль може знати лише IT-персонал, відповідальний за розробку та експлуатацію програмного забезпечення для обробки даних, а також Генеральний директор, якщо це необхідно для виконання їх обов'язків у Контролера даних. Комп'ютери, які використовуються для обробки даних, не повинні залишатися без нагляду в стані, придатному для введення або отримання даних.

Контролер даних може використовувати лише систему управління даними, яка реєструє доступ до системи, і на основі записаних даних можна визначити, хто і коли вносив дані.

2.9.4. Правила перевірки працівників

2.9.4.1. Поштові відправлення

Пошта, що надходить на робоче місце і якщо є припущення, що вона є особистою (наприклад, вказано "с.к." або точне ім'я отримувача), повинна бути передана співробітнику. Якщо лист з такою позначкою все ж відкривається, він має бути запечатаний, а на ньому повинна бути зазначена дата відкриття та ім'я особи, яка мала доступ до його вмісту.

2.9.4.2. Перевірка використання телефонів

Мобільні та стаціонарні телефони, надані Контролером даних працівникам, можуть використовуватись переважно для службових цілей, при цьому допускається обмежене особисте використання за умови пропорційного використання ресурсів.

Якщо Контролер даних як роботодавець хоче здійснювати моніторинг використання телефону працівниками на підставі своїх законних інтересів, це може стосуватися лише службового використання; моніторинг особистого використання заборонено. Як загальне правило, Контролер даних забезпечує присутність працівника під час перевірки та діє відповідно до принципу поступовості. До проведення перевірки роботодавець повинен поінформувати працівника про обставини обробки. Якщо контроль роботодавця стосується перевірки журналу дзвінків працівника, у такому випадку необхідно звернутися до постачальника телекомунікаційних послуг, щоб отримати детальний журнал дзвінків для відповідного телефонного номера, таким чином, щоб останні три цифри телефонних номерів у журналі дзвінків були анонімізовані, щоб працівник міг вибрати свої особисті дзвінки. Доступ до цього анонімізованого журналу дзвінків мають лише сам працівник і уповноважений представник роботодавця.

2.9.4.4. Повернення мобільного телефону співробітником

У разі, якщо співробітник повертає мобільний телефон, який використовував протягом трудових відносин або після їх припинення, необхідно забезпечити, щоб будь-які приватні дані, що зберігаються на пристрої (наприклад, номери телефонів, повідомлення, фотографії, відео, інші дані в будь-якій формі та змісті), могли бути зроблені резервні копії співробітником і потім безповоротно видалені. Співробітник повинен надати письмову заяву про видалення приватного вмісту у формі та змісті, зазначених у Додатку 7 до цих Регламентів. Пристрій може бути переданий третій стороні лише після того, як відповідальна особа за звільнення пристрою переконається, що на ньому немає або не може бути знайдено приватних даних. Особа, яка проводить цю процедуру, повинна дотримуватися зобов'язань з конфіденційності щодо розкритих приватних даних і не має права розголошувати ці дані або будь-яку інформацію, що стосується їх, третім особам.

2.9.4.3. Політика конфіденційності щодо використання та контролю електронних поштових скриньок

Електронна пошта, надана для робочих цілей, надається співробітнику Контролером даних для офіційного використання і не може бути використана для приватних цілей.

IT-відділ Контролера даних, відповідальний за безпечну роботу IT-систем, має право визначати обсяг пам'яті для вхідних повідомлень електронної пошти, обмежувати розмір та формат файлів, що додаються до листів, і інформувати співробітників про ці налаштування електронною поштою за необхідності, але не рідше ніж кожні шість місяців. Співробітники повинні дотримуватися цих налаштувань і будь-яких додаткових правил користування, встановлених відділом.

Співробітник може відкрити і використовувати додаткові неслужбові електронні поштові скриньки на робочому комп'ютері за умови, що таке приватне використання не завдасть шкоди бізнес-інтересам і репутації Контролера даних.

Контролер даних, як роботодавець, може на підставі свого законного інтересу контролювати офіційну кореспонденцію співробітника відповідно до положень цієї Політики. Під час перевірки Контролер даних зазвичай повинен забезпечити особисту присутність співробітника і діяти відповідно до принципу пропорційності. Перевірка повинна базуватися на результатах тесту на баланс інтересів, підготовленого Контролером. Роботодавець, який здійснює контроль, повинен письмово повідомити співробітника про конкретний інтерес, який перевіряється, до початку фактичної перевірки. Співробітник повинен повідомити роботодавця або особу, що діє від його імені, якщо електронна пошта містить персональні дані, до перегляду вмісту електронного листа під час перевірки. Контролер даних може без обмежень перевіряти вміст електронних листів, що стосуються робочих завдань.

Коли роботодавець бажає перевірити вміст офіційної поштової скриньки — на основі системи поетапного контролю — він має право попросити IT-відділ надати спочатку список заголовків листів. Цей список може включати одержувача, тему листа, тривалість відправки або отримання пошти, за необхідності додаткову інформацію, а також назву і розмір будь-якого доданого файлу.

Після ознайомлення зі списком роботодавець може призначити листи для доставки співробітнику, який має право відмовитися лише у разі, якщо лист є приватним. Роботодавець не має права знати вміст приватної кореспонденції. У випадку з приватною кореспонденцією, яка не є забороненою, знання вмісту листа не є необхідним для застосування будь-яких трудових правових наслідків щодо співробітника. Роботодавець має право вимагати від співробітника видалити таку кореспонденцію, і співробітник зобов'язаний виконати це прохання.

Якщо необхідну офіційну кореспонденцію потрібно сортувати з поштових скриньок, коли співробітник постійно відсутній на комп'ютері, співробітник може призначити іншого співробітника, який може зробити це за нього, увійшовши в поштову скриньку. Якщо це неможливо, керівник може призначити двох осіб, які, перебуваючи разом, можуть отримати з поштової скриньки лише зазначену офіційну пошту, але вони зобов'язані дотримуватися зобов'язань конфіденційності щодо неофіційної пошти і не розголошувати її вміст або будь-яку інформацію про неї керівнику або будь-яким іншим особам.

Якщо співробітник тимчасово відсторонений від роботи, його електронну пошту необхідно зробити недоступною (заблокувати) для співробітника та інших осіб на період відсторонення або на максимум три місяці після припинення трудових відносин, а також повинна бути впроваджена IT-настройка, яка повідомляє відправнику листа, надісланого на поштову адресу скриньки, автоматичною відповіддю, що:

- поштова скринька більше не використовується, і
- якщо ви хочете надіслати офіційну кореспонденцію до Контролера даних, вказати, на яку електронну чи поштову адресу.

Після цього строку електронна адреса поштової скриньки повинна бути зроблена неактивною, тобто повинна бути впроваджена IT-настройка, що забороняє отримання подальших листів.

2.9.4.4. Політика щодо електронних поштових скриньок співробітників

У вищезазначеній інформації не можна надавати дані або інформацію про причину припинення використання електронної поштової скриньки або про те, чи було припинено трудові відносини з відповідним співробітником, і якщо так, то з якої причини.

Окрім того, що електронна пошта має бути зроблена недоступною або неактивною, заборонено використовувати будь-які налаштування, які автоматично переспрямовують електронні листи зі скриньки на іншу електронну адресу.

Співробітник повинен мати можливість забрати будь-яку приватну кореспонденцію з його/її поштової скриньки у останній день роботи, але не пізніше ніж п'ять робочих днів після цієї дати. Цей процес збереження може бути перевірений призначеною особою лише за умови, що причина припинення трудових відносин виправдовує таку перевірку. У такому випадку призначена особа зобов'язана дотримуватись конфіденційності щодо приватних даних, про які вона дізнається.

Якщо пошта містить офіційну кореспонденцію такого характеру, що може бути необхідною для виконання майбутніх завдань і отримання документів призведе до надмірних труднощів для Контролера даних, поштову скриньку можна продовжувати використовувати після того, як всі приватні дані будуть вилучені та безповоротно видалені, і співробітник має бути про це проінформований. В майбутньому у поштовій скриньці можуть оброблятися лише офіційні листи.

2.9.4.4.4 Правила захисту даних щодо використання і контролю Інтернету співробітниками

Основною метою наданого співробітникам підключення до Інтернету є сприяння ефективній роботі, а приватне використання послуги дозволяється без шкоди для бізнес-інтересів і репутації Контролера даних і без надмірного обмеження потужностей IT-системи.

IT-відділ Контролера даних, відповідальний за безпечну роботу IT-систем, має право обмежувати використання Інтернету і визначати ключові слова, які IT-система автоматично відхиляє при доступі до вебсайтів, що їх містять. Ці правила викладені в відповідних внутрішніх правилах.

Якщо є обґрунтовані підстави підозрювати, що співробітник використовує Інтернет-з'єднання з порушенням вищезазначених правил, роботодавець повинен, як правило, з'ясувати обставини порушення шляхом особистої бесіди.

У разі неуспішності вищезазначеної процедури роботодавець може звернутися до IT-організації з проханням надати йому список вебсайтів, що були доступні на комп'ютері відповідного співробітника. У цьому випадку правовою підставою для обробки є законний інтерес роботодавця, що ґрунтується на проведеному тесті на баланс інтересів. Роботодавець має право, як правило, перевіряти цей список в присутності співробітника та обробляти неформальні дані тільки в обсязі та на строк, необхідний, без можливості детального ознайомлення з ними, і лише до того рівня, який необхідний для з'ясування можливих наслідків у трудовому праві.

2.9.4.5. Контроль робочого місця співробітника

Зона, де працює співробітник, така як його/її робочий стіл чи шафа, не може бути перевірена з метою контролю трудових відносин. Якщо виникає необхідність провести перевірку з інших цілей, така перевірка може бути проведена лише за умови, що відповідні правові положення дозволяють це і що Офіцер із захисту даних (DPO) дав попереднє схвалення. У будь-якому випадку співробітник має бути повністю поінформований про обробку даних, яка буде здійснюватися у зв'язку з перевіркою.

2.10. ВІДПОВІДАЛЬНІСТЬ

2.10.1 Загальні вимоги до управління та обробки даних.

Особа, яка має правовідносини з Контролером даних (особистий обсяг) і яка отримує особисті дані або обробляє їх на підставі своєї посади або функцій, зобов'язана захищати і охороняти ці дані, докладаючи всіх зусиль для забезпечення їх належного захисту.

Дані повинні бути захищені, зокрема, від несанкціонованого доступу, зміни, розкриття, передачі, знищення або знищення, випадкового знищення або пошкодження, а також від недоступності, що виникає через зміни у використаних технологіях.

Особи, які мають правовідносини з Контролером даних або діють від його імені, зобов'язані зберігати конфіденційність усіх особистих даних, що стали їм відомі в рамках їхніх правовідносин.

Особи, які мають правовідносини з Контролером даних і які здійснюють обробку даних або операції з обробки, несуть відповідальність за будь-які збитки, що виникають через порушення їхніх зобов'язань з обробки або захисту даних.

Коли обробка здійснюється від імені Контролера, Контролер може використовувати лише обробників, які надають достатні гарантії для впровадження відповідних технічних та організаційних заходів для забезпечення відповідності вимогам обробки та захисту прав суб'єктів даних.

Обробка, що здійснюється обробником, регулюється контрактом, який зобов'язує обробника діяти від імені Контролера. Контракт має бути укладений виключно в письмовій формі.

Контракт має містити зокрема:

a) ідентифікацію Контролера даних і Обробника даних;

b) предмет обробки;

c) тип особистих даних, що підлягають обробці;

d) кількість особистих даних, що підлягають обробці (за можливості);

e) категорії осіб, яких це стосується;

f) характер і мета обробки;

g) правова підстава для обробки;

h) тривалість обробки;

i) що робити після завершення надання послуг обробки;

j) обов'язки та права Контролера даних;

k) обробник обробляє особисті дані виключно на підставі письмових інструкцій Контролера, зокрема щодо передачі особистих даних до третіх країн або міжнародних організацій, якщо тільки обробка не є вимогою законодавства Союзу чи держави-члена, у такому випадку обробник має повідомити Контролера про це правове зобов'язання до початку обробки, якщо інше не заборонено відповідним законодавством з огляду на важливі публічні інтереси;

l) спосіб надання інструкцій або підтримки контактів між Контролером і Обробником;

m) рішення про використання додаткового обробника;

n) Обробник дотримується правових вимог щодо використання додаткового обробника;

o) конфіденційність;

p) вимоги до безпеки даних;

q) допомога у виконанні стандартів безпеки даних, управлінні інцидентами та оцінках впливу;

r) допомога в реалізації прав суб'єктів даних;

s) надання інформації Контролеру даних і право Контролера на контроль;

t) метод здійснення контролю Контролером даних;

u) певні питання відповідальності;

v) засоби забезпечення виконання.

У разі необхідності, Контролер і Обробник повинні вжити додаткових заходів для забезпечення того, щоб фізичні особи, які мають доступ до особистих даних і діють під владою Контролера або Обробника, обробляли ці дані лише відповідно до інструкцій Контролера.

2.10.2. Вимоги до передачі даних

В межах організаційної системи Контролера даних особисті дані можуть передаватися — в обсязі та на період, необхідний для виконання завдання — організаційній одиниці або особі, чий доступ до персональних даних і їх обробка необхідні для виконання завдання, що здійснюється Контролером даних.

Обробка даних з різними цілями може бути об'єднана Контролером даних лише відповідно до законних цілей і коли це обґрунтовано.

Запит на передачу персональних даних, що обробляються Контролером даних, може бути виконаний лише на підставі правового вимогу або якщо виконуються умови, визначені наступним абзацом. В усіх інших випадках передача повинна бути відмовлена.

У випадках, коли передача не є зобов'язанням за законом, запит може бути виконаний тільки в разі надання суб'єктом даних своєї згоди після того, як він був детально поінформований і це підтверджено, або якщо це необхідно для цілей законних інтересів, що переслідуються Контролером даних або третьою стороною.

У випадку передачі даних за кордон, експортер даних повинен спеціально перевірити, чи виконуються умови для передачі даних за кордон, зазначені в GDPR. Це має включати оцінку того, чи відповідає передача одному з правових підстав, встановлених у GDPR, і чи забезпечено належний рівень захисту даних отримувачем даних. Якщо передача відбувається до держави-члена Європейської економічної зони, оцінка належного рівня захисту персональних даних не є необхідною.

Передача персональних даних, включаючи перепередачу персональних даних з третьої країни чи міжнародної організації в іншу третю країну або іншу міжнародну організацію, які обробляються після їх передачі до третьої країни чи міжнародної організації, може мати місце лише за умови, що і Контролер, і Обробник дотримуються умов, визначених у GDPR.

Передача персональних даних до третьої країни чи міжнародної організації може відбутися, якщо Європейська Комісія ухвалила або опублікувала в Офіційному журналі Європейського Союзу та на своєму вебсайті, що третя країна, територія чи один або кілька конкретних секторів третьої країни чи міжнародна організація забезпечують належний рівень захисту (рішення про адекватність). Для таких передач не потрібна окрема авторизація.

При передачі персональних даних поштою необхідно забезпечити, щоб пошта була запечатана.

Контролер даних зобов'язується надавати персональні дані для статистичних цілей лише так, щоб їх не можна було пов'язати з конкретним суб'єктом даних.

Контролер даних зберігає реєстр всіх передач даних, що здійснюються ним, відповідно до реєстру, наведеного в Додатку 6 до Правил.

2.10.3. Реєстри обробки діяльності

Контролер зобов'язаний вести реєстри всіх своїх діяльностей з обробки, які: (a) можуть призвести до ризику для прав та свобод суб'єктів даних; b) не є випадковими; c) включають обробку чутливих даних або персональних даних, що стосуються кримінальних правопорушень. Контролер даних має виконувати вище вказану вимогу щодо ведення реєстрів відповідно до вмісту Додатку 3 до цієї Політики конфіденційності. Адміністратор, який здійснює обробку, виконує обов'язок вести реєстри від імені Контролера відповідно до цього пункту. Генеральний директор забезпечує, щоб реєстри заходів з охорони даних підтримувалися в актуальному стані.

Виконавчий директор надасть реєстр органу NAIH за запитом.

Записи діяльності з обробки даних включають:

a) назву та контактні дані Контролера даних;

b) опис обробки;

c) реальне місце обробки;

d) мету обробки;

e) правову основу обробки;

f) правову основу обробки (повторюється);

g) у разі спільної обробки — назву та контактні дані спільного контролера;

h) місце обробки;

i) дії обробника щодо обробки;

j) технології обробки даних;

k) назву IT-застосунку;

l) обсяг особистих даних, що обробляються контролером;

m) тривалість обробки;

n) джерело даних;

o) у разі передачі — тип даних;

p) назву та контактні дані отримувача;

q) у разі передачі особистих даних до третьої країни або міжнародної організації — інформацію щодо відповідних заходів безпеки;

r) правову основу передачі;

s) обсяг зацікавлених осіб;

t) опис технічних та організаційних заходів, вжитих для забезпечення безпеки даних.

2.11. ОРГАНІЗАЦІЯ ВНУТРІШНІХ ТРЕНІНГІВ, ТРЕНІНГІВ З GDPR ТА РОЗВИТОК ОБІЗНАНОСТІ ПРО ЗАХИСТ ДАНИХ У РАМКАХ РОБОЧОЇ ОРГАНІЗАЦІЇ, РЕГУЛЯРНІ ВНУТРІШНІ ПРОЦЕСИ АУДИТУ ЗАХИСТУ ДАНИХ

Відповідно до вимог щодо організації обізнаності про дані, Компанія приділяє велике значення важливості принципів і правил захисту даних у всіх сферах своєї діяльності та підвищенню обізнаності про них у межах організації. Згідно зі статтею 39 GDPR, DPO (офіцер із захисту даних) має здійснювати нагляд за дотриманням GDPR та інших європейських або національних положень про захист даних, а також внутрішніх правил контролера чи обробника даних, які стосуються захисту персональних даних, включаючи призначення відповідальних осіб, підвищення обізнаності та навчання співробітників, що беруть участь в обробці даних, а також проведення відповідних аудитів. Якщо DPO не призначений, Компанія організовує необхідне навчання для підвищення обізнаності співробітників.

2.11.1 Структура внутрішнього навчання

Для підвищення обізнаності про захист даних Компанія застосовує наступну систему навчання та звітування про знання для своїх колег, які здійснюють операції з обробки даних у межах своєї роботи.

2.11.1.1.1. Навчання з конфіденційності при вступі

Протягом 10 днів після вступу до Компанії співробітники проходять обов'язкове навчання з обізнаності про захист даних, яке включає наступні обов'язкові теми: концепція персональних даних, концепція та правова основа обробки даних, ризик захисту даних, оцінка ризиків, обізнаність про дані у повсякденному бізнесі, обов'язок повідомляти про інциденти, основні види обробки даних у Компанії.

2.11.1.2.2. Щорічне навчання з обізнаності про захист даних

Обов'язкове відвідування хоча б одного організованого централізовано тренінгу на рік, щоб забезпечити підтримку обізнаності про захист даних, є обов'язковим для всіх співробітників, що працюють з персональними даними. Тренінг може бути організований всередині компанії, але також можна використовувати сторонніх постачальників послуг.

2.11.1.3. Щорічний тест для оцінки готовності до захисту даних

Протягом 14 днів після відвідування обов'язкової щорічної презентації всі співробітники, що працюють з персональними даними, повинні пройти онлайн-тест для оцінки їх знань у сфері захисту даних. Тест вважається успішно пройденим, якщо співробітник набирає не менше 80%. У відповідності до цього тест повинен бути пройденим, поки не буде досягнуто вимоги 80%.

2.11.2 Інші положення

Компанія переглядатиме та оновлюватиме навчальні матеріали та тест на знання з захисту даних, на основі якого побудована система навчання, щорічно, централізовано, під керівництвом офіцера з захисту даних (якщо такий є), а за необхідності з допомогою експертів, відповідно до статті 39 (1) (b) GDPR.

2.12. ОБРОБКА ІНЦИДЕНТІВ З ПОРУШЕННЯМ ЗАХИСТУ ДАНИХ

Порушення захисту даних — це порушення безпеки, яке призводить до випадкового або незаконного знищення, втрати, змін, несанкціонованого розкриття або доступу до персональних даних, що передаються, зберігаються або обробляються іншим способом.

Порушення захисту даних може спричинити фізичні, грошові або немайнові збитки для суб'єктів даних (та, опосередковано, для Компанії), якщо з ним не буде вчасно та належним чином впоратися. Такі збитки можуть включати, але не обмежуються ними, втрату контролю над їх персональними даними (коли несанкціоновані особи отримують доступ до даних і неможливо визначити, для чого вони будуть використані), фінансові збитки (наприклад, крадіжка даних кредитної картки), шкоду репутації, витік конфіденційної бізнес-інформації тощо.

Приклади найбільш поширених інцидентів включають: втрату ноутбука, мобільного телефону, носіїв даних, що містять персональні дані, відправку персональних даних на неправильну електронну адресу, небезпечне зберігання персональних даних (наприклад, платіжні квитанції, викинуті в сміття); небезпечну передачу даних, несанкціоноване копіювання або передачу списків клієнтів та партнерів, атаки на сервери, злам вебсайтів.

2.12.1. Виявлення порушення захисту даних

Контролер даних може бути повідомлений про неочікувану подію або внутрішнім, або зовнішнім сигналом.

Внутрішній сигнал вважається неочікуваною подією, якщо особа, яка перебуває у трудових чи інших правових відносинах з Контролером даних або обробником даних, що діє на основі договору з Контролером даних, дізнається про неочікувану подію.

Якщо особа, яка перебуває у трудових чи інших правових відносинах з Контролером даних, помітила неочікувану подію, вона повинна негайно, але не пізніше ніж через 2 години з моменту виявлення, повідомити про це безпосереднього керівника або керівника Контролера даних.

Якщо особа, яка перебуває в трудових чи інших правових відносинах з Контролером даних і не має безпосереднього керівника, дізнається про неочікувану подію, вона повинна негайно повідомити керівника Контролера даних, але не пізніше ніж через 2 години після виявлення.

Якщо обробник даних, який діє на підставі договору з Контролером даних, дізнається про неочікувану подію, він повинен без затримки повідомити про це керівника Контролера даних через контактну особу, вказану в згаданому договорі, але не пізніше ніж через 2 години після виявлення.

Зовнішній сигнал вважається повідомленням, якщо будь-яка особа, яка не входить до вищезазначених категорій, дізнається про неочікувану подію і повідомляє про неї Контролера даних усно, письмово або електронно.

2.12.2. Розслідування порушення захисту даних

Якщо зовнішній сигнал отримано особою, яка перебуває в трудових або інших правових відносинах з Контролером даних, ця особа повинна без затримки, але не пізніше ніж через 2

години після виявлення інциденту, повідомити свого безпосереднього керівника або керівника Контролера даних.

Якщо інформація надійшла до особи, яка перебуває в трудових або інших правових відносинах з Контролером даних і не має безпосереднього керівника, ця особа повинна без затримки, але не пізніше ніж через 2 години після виявлення інциденту, повідомити керівника Контролера даних.

Якщо інформація надійшла до обробника даних, що діє на підставі договору з Контролером даних, обробник повинен без затримки повідомити керівника Контролера даних через контактну особу, зазначену в цьому договорі, але не пізніше ніж через 2 години після виявлення інциденту.

Будь-який запит, надісланий НАЗІХ до Контролера даних, вважається зовнішнім сигналом.

Керівник Контролера даних повинен без затримки розглянути отриману інформацію про неочікувану подію. При цьому він повинен врахувати наступні фактори:

- чи пов'язана неочікувана подія з персональними даними;
- чи була неочікувана подія результатом порушення безпеки;
- який наслідок для персональних даних мало порушення безпеки.

В рамках розслідування неочікуваної події керівник Контролера даних має право запитувати інформацію у особи, яка перебуває в трудових відносинах з Контролером даних, у будь-якої іншої особи, яка перебуває в трудових або інших правових відносинах з Контролером даних, а також у обробника даних, що діє на підставі договору з Контролером даних.

Якщо в результаті проведеного розслідування керівник Контролера даних встановлює, що неочікувана подія, що стосується персональних даних, сталася внаслідок порушення безпеки, це вважається встановленням факту знання відповідно до статті 33(1) GDPR.

Якщо в результаті розслідування керівник Контролера даних визначає, що неочікувана подія є порушенням захисту даних, він/вона також має категоризувати інцидент.

2.12.3. Проведення розслідування порушення захисту даних

Керівник Контролера даних має без затримки, але не пізніше ніж через 2 години після виявлення інциденту, скликати Команду управління інцидентами.

Команда управління інцидентами відповідає за розслідування обставин порушення захисту даних, оцінку, аналіз та управління ризиками порушення, а також за прийняття рішень щодо подальших дій у зв'язку з порушенням.

Команду управління інцидентами очолює та керує керівник Контролера даних.

Команда управління інцидентами буде збиратися регулярно, відповідно до визначеного керівником Контролера даних графіку, до завершення обробки інциденту захисту даних.

Команда управління інцидентами буде розпущена після завершення обробки інциденту захисту даних, включаючи будь-які рішення, прийняті в рамках процедури НАЗІХ.

По завершенню своєї діяльності команда управління інцидентами підготує звіт для виконавчого керівника Контролера даних про обробку інциденту у формі та змісті, зазначених у Додатку 8 до цих Правил.

Члени команди управління інцидентами:

- директор з інформаційних технологій;
- юридичний представник компанії;
- колега особи, що постраждала;
- генеральний директор Контролера даних або особа, уповноважена генеральним директором.

Команда управління інцидентами може включати інших осіб за потреби.

Перше засідання команди управління інцидентами відкриває керівник Контролера даних.

На першому засіданні команди управління інцидентами керівник Контролера даних представить наявну інформацію та факти про порушення захисту даних, зокрема обставини, за яких сталося порушення захисту даних, та категоризацію порушення.

Після цього команда управління інцидентами почне оцінювати та аналізувати ризики інциденту, враховуючи їх ймовірність і серйозність. Ризики мають оцінюватися з точки зору їхнього джерела, середовища обробки, персональних даних та потенційного впливу інциденту.

(4) Фактори, які можуть бути враховані при визначенні джерела ризиків:

a) інцидент є наслідком ненавмисної внутрішньої поведінки чи діяльності;

b) інцидент є наслідком навмисної внутрішньої поведінки чи діяльності;

c) інцидент є наслідком ненавмисної зовнішньої поведінки чи діяльності;

d) інцидент є наслідком навмисної зовнішньої поведінки чи діяльності.

(5) Фактори, які повинні бути враховані для оцінки середовища, у якому сталося порушення:

a) засоби обробки даних (на паперових носіях або автоматизовані);

b) система, що була залучена до інциденту (поштові системи, носії даних тощо);

c) заходи для захисту безпеки серверного середовища (наприклад, шифрування, іменування, брандмауери);

d) стійкість серверного середовища;

e) ефективність заходів, вжитих заздалегідь для запобігання інциденту;

f) фактори, що сприяли виникненню інциденту;

g) інші фактори, що вплинули на виникнення інциденту;

h) ймовірність відновлення функціонування системи.

(6) Фактори, які можуть бути враховані при оцінці особистих даних:

a) категорії особистих даних, зокрема чутливі дані;

b) кількість особистих даних;

c) категорії осіб, яких це стосується, зокрема їх уразливість (діти, працівники);

d) ідентифікація суб'єктів даних;

e) кількість осіб, яких це стосується.

(7) Фактори, які повинні бути враховані при оцінці впливу інциденту:

a) фізичні ушкодження або небезпека;

b) майнові збитки;

c) немайнові збитки.

Команда управління інцидентами повинна класифікувати інцидент відповідно до рівня ризику, а саме: низький, середній або високий ризик.

Велика кількість випадків, зазначених у пунктах 4(b) до (d), наявність уразливих суб'єктів даних відповідно до пунктів 6(a) та (c), суб'єктів особистих даних згідно з пунктом 6(b) і суб'єктів даних, згідно з пунктом 6(e), повинна розглядатися як середній або високий ризик.

Також ймовірно існує високий ризик для прав і свобод фізичних осіб, якщо порушення призведе до:

a) дискримінації стосовно особи, якої це стосується;

b) крадіжки ідентичності;

c) фінансових втрат;

d) пошкодження репутації особи, якої це стосується;

e) порушення конфіденційності особистих даних, захищених професійною таємницею;

f) розблокування псевдонімізації без дозволу;

g) будь-яких інших значних економічних або соціальних збитків;

h) неможливості здійснювати свої основні права чи свободи;

i) втрати права суб'єктів даних на здійснення своїх виборів щодо їх особистих даних;

j) оцінки особистих характеристик з метою створення або використання особистого профілю.

У випадку, коли порушення даних є низьким ризиком, вважається малоймовірним, що це порушить права та свободи фізичних осіб.

У випадку, коли порушення даних є середнім ризиком, вважається ймовірним, що це призведе до ризику для прав і свобод фізичних осіб, відповідно до статті 33(1) Загального регламенту захисту даних (GDPR).

У випадку, коли порушення даних є високим ризиком, це вважається ймовірним, що це призведе до високого ризику для прав і свобод фізичних осіб, відповідно до статті 34(1) GDPR.

Команда управління інцидентами також повинна вжити всіх необхідних заходів для пом'якшення або запобігання наслідкам порушення даних, зокрема відновлення функціонування постраждалих систем, інформування суб'єктів даних (якщо це необхідно), а також, у разі порушення або злочину, повідомлення компетентних органів для розслідування порушення чи злочину.

2.12.3. Повідомлення про порушення даних

Якщо порушення особистих даних, ймовірно, призведе до ризику для прав і свобод фізичних осіб, Контролер даних зобов'язаний без зайвих зволікань повідомити НАЗК (Національний орган з захисту персональних даних), і, за можливості, не пізніше ніж через 72 години після того, як стало відомо про порушення особистих даних.

Якщо обставини інциденту та оцінка ризиків це виправдовують, повідомлення може бути подано частинами. Обов'язок повідомлення від імені Контролера даних виконуватиме Генеральний директор. Генеральний директор надасть повідомлення на папері або через електронну систему повідомлень, доступну на вебсайті НАЗК.

Повідомлення до НАЗК повинно містити:

a) дані Контролера даних;

b) дату порушення даних;

c) дату, коли стало відомо про порушення даних;

d) спосіб виявлення порушення даних;

e) причини затримки у наданні інформації;

f) характер порушення даних;

g) особисті дані, що стали об'єктом порушення;

h) орієнтовну кількість особистих даних, на які вплинуло порушення;

i) категорії осіб, яких це стосується;

j) заходи, вжиті до порушення даних;

k) наслідки порушення даних;

l) фізичні, матеріальні чи нематеріальні збитки або інші значні наслідки для суб'єктів даних та серйозність ймовірних наслідків;

m) вжиті заходи;

n) заходи, вжиті для виправлення порушення даних;

o) інші повідомлення;

p) ім'я та контактні дані Офіцера з захисту даних (DPO).

Усі працівники Контролера даних зобов'язані співпрацювати з НАЗК у рамках процедур, що ініціюються у зв'язку з обробкою порушень даних.

Генеральний директор зобов'язаний надати НАЗК всю необхідну інформацію для ведення процедур, пов'язаних з обробкою порушень даних.

Для виконання цього обов'язку Генеральний директор має право запитувати інформацію від осіб, які перебувають у трудових або інших правових відносинах з Контролером даних, а також від обробника даних, який діє на підставі договору з Контролером даних.

Члени команди управління інцидентами повинні співпрацювати з Офіцером з захисту даних у виконанні цього обов'язку.

Якщо повідомлення не було подано, Контролер даних повинен задокументувати причини, через які повідомлення не було подано.

Інформація про те, чи було подано повідомлення, стане частиною звіту команди управління інцидентами.

2.12.4. Інформація для суб'єктів даних

Якщо порушення персональних даних може призвести до високого ризику для прав і свобод людини і громадянина

2.12.4. Інформування суб'єктів даних про порушення

Якщо порушення особистих даних, ймовірно, призведе до ризику для прав і свобод фізичних осіб, Контролер даних зобов'язаний без зайвих зволікань інформувати суб'єкта даних про порушення особистих даних.

Обов'язок інформувати суб'єкта даних згідно з пунктом 1 виконує Офіцер з захисту даних від імені Контролера даних.

У випадку, коли порушення особистих даних стосується осіб, що працюють у Контролера даних, інформація надається через системи, що використовуються для зв'язку з працівниками, з залученням відділів, які працевлаштовують суб'єктів даних.

У випадку порушення особистих даних, що стосується осіб, не охоплених пунктом 3, інформація надається за допомогою систем, що використовуються для комунікації з суб'єктами даних. У цьому випадку, прес-служба Контролера допомагає у розробці змісту інформації.

У випадках, коли через велику кількість суб'єктів даних надання персональної інформації неможливе або є непропорційно обтяжливим для Контролера даних, інформація може бути надана також за допомогою оголошення в місцевих або національних ЗМІ.

У випадках, зазначених у попередніх двох пунктах, на вебсайті Контролера буде розміщено сповіщення, яке надасть загальну інформацію про характер інциденту, особисті дані, що були порушені, та категорії суб'єктів даних.

Інформація, надана суб'єкту даних або суб'єктам даних, повинна включати принаймні:

a) опис характеру порушення даних;

b) ім'я та контактні дані Офіцера з захисту даних;

c) опис ймовірних наслідків порушення даних;

d) опис вжитих або передбачених заходів для усунення порушення особистих даних, включаючи, де це доцільно, заходи для пом'якшення будь-яких негативних наслідків порушення;

e) опис заходів, які суб'єкти даних можуть вжити для усунення порушення особистих даних, включаючи, де це доцільно, заходи для пом'якшення будь-яких негативних наслідків порушення.

Для виконання цього обов'язку Генеральний директор має право запитувати інформацію від осіб, що перебувають у трудових або інших правових відносинах з Контролером даних, а також від обробників даних, які діють на підставі договору з Контролером.

Члени команди управління інцидентами зобов'язані співпрацювати з Генеральним директором у виконанні цього обов'язку щодо інформування.

Якщо інформація не була надана, Генеральний директор зобов'язаний задокументувати причини, чому інформація не була надана.

Інформація про те, чи була надана інформація, стане частиною звіту команди управління інцидентами.

2.12.5. Реєстрація порушення даних

Контролер даних зобов'язаний вести облік порушень даних, незалежно від їх класифікації за ризиком.

Контролер даних має виконувати своє зобов'язання згідно з попереднім абзацом у формі та змісті, зазначених в Додатку 9 до цієї Політики.

Записи про інциденти з порушенням захисту даних повинні включати:

a) ім'я та контактні дані Контролера даних;

b) ідентифікатор порушення даних;

c) обсяг порушених особистих даних;

d) суб'єкти даних, яких стосується порушення;

e) кількість осіб, яких стосується порушення;

f) дата, коли сталося порушення даних;

g) дата, коли стало відомо про порушення даних;

h) характер порушення даних;

i) обставини порушення даних;

j) вплив порушення даних;

k) вжиті заходи для реагування на порушення даних;

l) інші дані, визначені законодавством, що регулює обробку даних;

m) факт зобов'язання повідомити;

n) дата офіційного повідомлення;

o) ім'я особи, яка здійснила повідомлення;

p) факт зобов'язання інформувати;

q) дата, коли були поінформовані суб'єкти даних;

r) дата внесення запису.

Генеральний директор виконує обов'язок щодо реєстрації від імені Контролера даних. Генеральний директор має забезпечити актуальність та оновлення записів про інциденти з порушенням захисту даних.

Генеральний директор надає реєстр на запит НАЗК.

2.13. ВНУТРІШНІ ПРАВИЛА, ЯКІ ПОВИННІ ДОТРИМУВАТИСЯ ПРИ ДІЇ АДМІНІСТРАТИВНОГО ОРГАНУ

Генеральний директор (відповідальна особа) несе основну відповідальність за забезпечення належної співпраці з органом влади в межах організації компанії. Будь-який запит від органу влади має бути негайно переданий відповідальній особі для подальшої обробки. Генеральний директор, у консультації з юридичним представником компанії, може, за необхідності, в

залежності від характеру запиту, ініціювати створення внутрішньої робочої групи або залучення зовнішнього експерта.

У всіх випадках необхідно відповісти на запит органу влади в межах встановленого строку, надавши всі запитувані дані/інформацію/документи. Зміст будь-якого документа, що надсилається органу влади, має бути затверджений Генеральним директором.

1. Додаток 1 - Форма тесту для оцінки зацікавленості

ТЕСТ НА ОЦІНКУ ЗАЦІКАВЛЕНОСТІ	
Назва компанії:	
Предмет тесту на інтерес	
Підготував (ім'я, посада)	
Затверджено (ПІБ, посада)	
Дата підготовки	
Дата затвердження	
Номер журналу	
Мета передбаченої обробки	
Правова основа для передбаченої обробки (відповідність GDPR)	
Обсяг персональних даних, які підлягають обробці	
Джерело персональних даних	
Тривалість обробки	
Гарантії, надані Компанією	

ВИСНОВКИ	
Законний інтерес Компанії	
Необхідність обробки	
Порушення прав і свобод суб'єктів даних	
Баланс інтересів	

Зроблено за адресою: Будапешт, 20.....

Генеральний директор

2. Додаток 1 - Процес оцінки ризиків



2. Додаток 1 - Реєстр управління даними

ДІЯЛЬНІСТЬ З ОБРОБКИ

Назва обробки даних	
Фактичне місце обробки [1]	
Мета обробки даних [2]	
Правова підстава для обробки даних	
Назва правової підстави для обробки	
Назва, адреса спільного контролера [3]	
Місце обробки[4]	
Діяльність обробника щодо обробки даних[5]	
Технологія обробки даних [6]	
Назва IT-додатку	
Обсяг персональних даних, які обробляє контролер [7]	
Тривалість обробки	
Джерело даних [8]	
Тип даних у разі передачі даних [9]	
Найменування адресата, повна адреса [10]	
Інформація про відповідні гарантії у разі передачі персональних даних третій стороні або міжнародній організації [11]	
Правова підстава для передачі [12]	
Кого це стосується [13]	
Опис технічних та організаційних заходів, вжитих для гарантування безпеки даних [14]	

[1] Адреса Контролера даних (якщо дані зберігаються в іншому місці, будь ласка, вкажіть її).
[2] Яка мета цих даних?
[3] Стаття 26 GDPR.
[4] Де дані записуються або зберігаються.
[5] Якщо є процесор даних, ви повинні вказати, яку діяльність він виконує. Наприклад: хостинг, розсилка, обслуговування веб-сайту.
[6] Вручну або за допомогою електронної інформаційної системи (IT-додаток, в електронному вигляді).
[7] Наприклад: ім'я, ім'я матері, адреса, адреса електронної пошти тощо.
[8] Дані надходять від суб'єкта даних чи від третьої особи або організації?
[9] У випадку передачі даних, коли дані виходять за межі компанії, які саме дані виходять (конкретно вказані, як у пункті 9)
[10] Тут також має бути вказана назва обробника даних, якому передаються дані.
[11] Чи передаються персональні дані до третьої країни (за межами ЄС)? І чому (будь ласка, вкажіть)?
[12] Наприклад, згода, договір.
[13] Люди похилого віку, родичі, бенефіціари, контактна особа, клієнти.
[14] Назва застосованих заходів захисту даних

Назва обробки даних	
Фактичне місце обробки	
Мета обробки даних	
Правова підстава для обробки даних	
Назва правової підстави для обробки	
Назва, адреса спільного контролера	
Місце обробки	
Діяльність обробника щодо обробки даних	
Технологія обробки даних	
Назва IT-додатку	
Обсяг персональних даних, які обробляє контролер	
Тривалість обробки	
Джерело даних	
Тип даних у разі передачі даних	
Ім'я одержувача, повна адреса	
Інформація про відповідні гарантії у разі передачі персональних даних третій країні або міжнародній організації	
Правова підстава для передачі	
Кого це стосується	
Опис технічних та організаційних заходів, вжитих для гарантування безпеки даних	

Назва обробки даних	
Фактичне місце обробки	
Мета обробки даних	
Правова підстава для обробки даних	
Назва правової підстави для обробки	
Назва, адреса спільного контролера	
Місце обробки	
Діяльність процесора щодо обробки даних	
Технологія для управління даними	
Назва IT-додатку	
Обсяг персональних даних, які обробляє контролер	

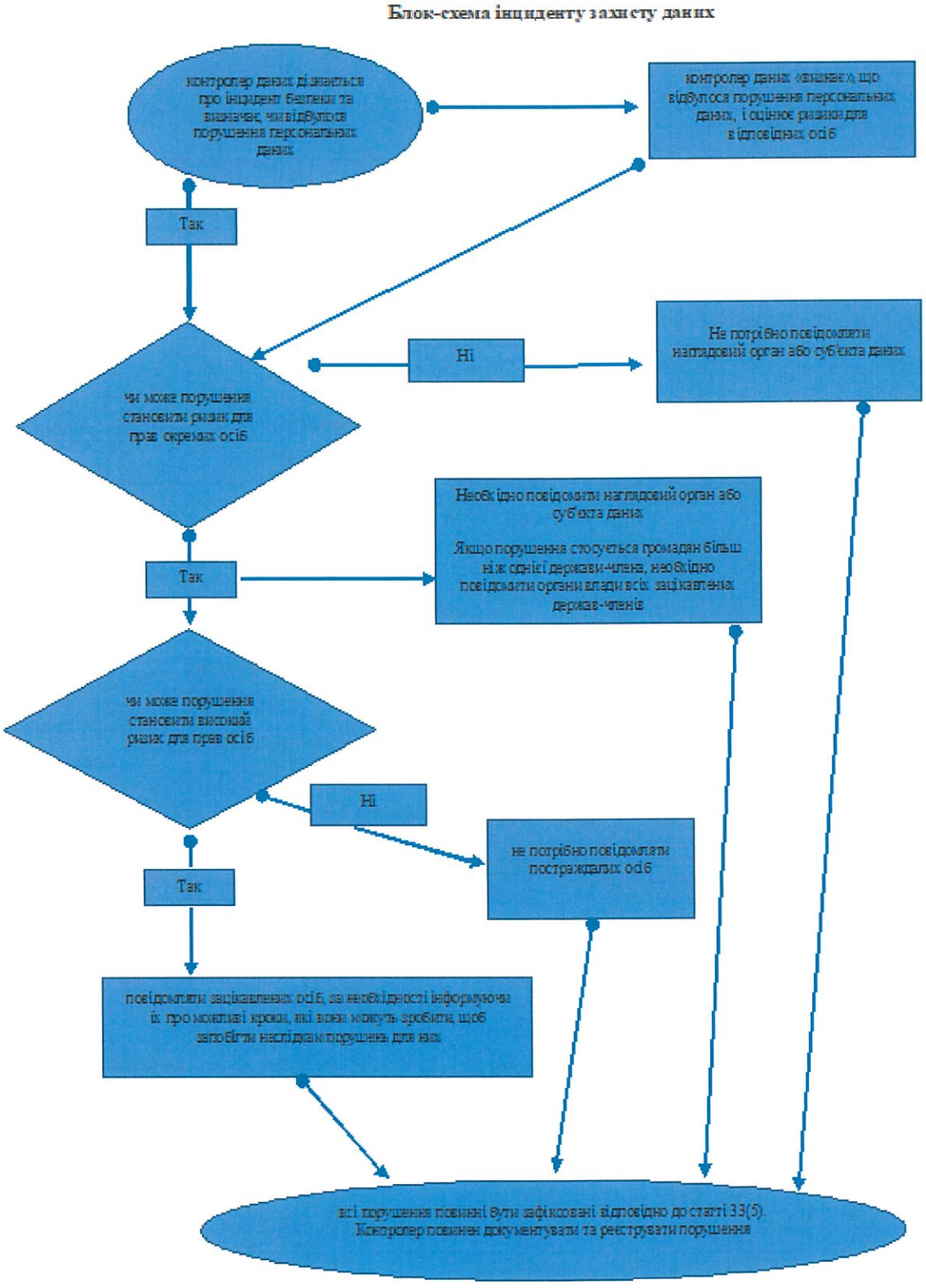
Тривалість обробки	
Джерело даних	
Тип даних у разі передачі даних	
Найменування адресата, повна адреса	
Інформація про відповідні гарантії у разі передачі персональних даних третій стороні або міжнародній організації	
Правова підстава для передачі	
Кого це стосується	
Опис технічних та організаційних заходів, вжитих для гарантування безпеки даних	

2. Додаток 1 - Політика конфіденційності

РЕЄСТРАЦІЯ ЗАПИТІВ СУБ'ЄКТІВ ДАНИХ

№	Ім'я та контактні дані суб'єкта даних, який бажає реалізувати своє право на доступ	Характер права на доступ, що запитується (зміст запиту)	Дата запиту на виконання	Правова підстава для обробки даних суб'єкта даних, який бажає реалізувати своє право на доступ	Заходи, вжиті для виконання запиту на виконання	Дата виконання запиту на виконання	Правові та фактичні підстави для вжиття заходів щодо обмеження або відмови у праві на доступ	Дата реєстрації, підпис реєстратора
1.								
2.								

2. **Додаток 1 - Блок-схема інциденту захисту даних** (Джерело: Робоча група із захисту даних - WP250rev01 - Керівні принципи)



2. **Додаток №.**

ЗАПИС ПЕРЕДАЧІ ДАНИХ

№	Дата передачі персональних даних	Назва підзвітного підрозділу	Правова підстава та мета передачі	Визначення обсягу переданих персональних даних	Одержувач передачі	Передача до третіх країн	Інші дані, визначені законодавством, що передбачає обробку, додаткова примітка	Дата внесення, ПІБ реєстранта, підпис
.								
.								
.								
.								
.								
.								
.								
.								

2. **Додаток №.**

Декларація про вміст даних IT-обладнання при його поверненні

Ім'я: ....., (ім'я матері: ....., місце народження: ....., дата народження: .....) Заявляю, що Закрите Товариство з обмеженою відповідальністю «EWG Customs Agency Services» (Реєстраційний номер: 01-10-141551; податковий номер: 26242387-2-41), як мій роботодавець, надало мені наступні інформаційно-комунікаційні пристрої (робочий комп'ютер, смартфон, інші IT та інформаційно-комунікаційні пристрої) з метою виконання завдань, пов'язаних з моєю роботою

назва пристрою: ID:

.....

.....

.....

.....

Я заявляю, що вищезазначені засоби містять лише дані, пов'язані з моїми робочими завданнями.

Дата і місто: .....,.....

.....

Працівник

Я отримав цю декларацію від імені компанії EWG Customs Agency Services Private Limited:

Дата і місто: .....,.....

.....

ПІБ, підпис

Додаток 8

ПРОТОКОЛ

ОБРОБКИ ВИТОКІВ ДАНИХ

Детальна інформація про конференцію		
Назва та мета зустрічі:	**Комітет із захисту даних, розслідування порушень даних**	
Дата та місце проведення: Номер протоколу:		
Особа, яка веде протокол:		
Імена учасників		**Посади, які займають учасники**

1. **Передісторія:**

2. **Класифікація події**

   - На підставі вищевикладеного можна зробити висновок, що інцидент, пов'язаний із захистом даних, стався/не стався (причина: ...)

3. **Характеристики порушення даних:**

   - Характер зацікавлених сторін:
   - Кількість постраждалих осіб:
   - Характер шкоди:
   - Характер порушення даних:
   - Причина порушення даних:
   - Обставини та наслідки порушення даних:
   - Опис заходів, вжитих до порушення даних:

- Наслідки порушення даних:
- Характер відповідних персональних даних:

4. Висновки та пропозиції

З огляду на характер і серйозність порушення даних, а також його наслідки та негативний вплив на суб'єкта даних, Комітет із захисту даних вирішив, що повідомлення до Органу захисту даних є/не є необхідним, і що порушення даних становить високий ризик для прав і свобод суб'єктів даних, тобто їхнього приватного життя.

2. Пропозиції Комітету з питань захисту даних:

а) ...

Відповідальні: ...

б) У сфері зменшення ризиків:

Відповідальний: ...

с) Інше

Відповідальний: ....

г) Кінцевий термін виконання: ...

Дата:

.....	.....	.....
ПІБ, посада	ПІБ, посада хронометрист	ПІБ, посада

.....

ПІБ, посада

Додаток 9 - Реєстр інцидентів у сфері захисту персональних даних

ПОРУШЕННЯ ДАНИХ

Серійний номер [15]	
Обсяг персональних даних, про які йдеться [16]	
Суб'єкти даних, яких торкнулося порушення даних[17]	
Кількість суб'єктів даних, яких торкнулося порушення даних	
Дата порушення даних	
Дата, коли стало відомо про порушення даних	
Характер порушення даних	
Обставини порушення даних	
Наслідки порушення даних	
Заходи, вжиті для реагування на порушення даних	
Інші дані, визначені законодавством, що передбачає обробку	
Чи повинен я повідомляти про це НОЗД?	
Дата публічного повідомлення	
Ім'я особи, яка повідомляє	
Чи потрібно інформувати зацікавлені сторони?	
Дата інформування зацікавлених сторін	
Дата реєстрації (рік, місяць, день)	

Серійний номер	
Обсяг персональних даних, про які йдеться	
Кого торкнулося порушення даних	
Кількість суб'єктів даних, яких торкнулося порушення даних	
Дата витоку даних	

[15] Заповнюється для кожного інциденту!
[16] Наприклад: ім'я, ім'я матері, адреса, адреса електронної пошти тощо.
[17] Наприклад, працівник тощо.

Дата, коли стало відомо про порушення даних	
Характер порушення даних	
Обставини порушення даних	
Наслідки порушення даних	
Заходи, вжиті для реагування на порушення даних	
Інші дані, визначені законодавством, що передбачає обробку	
Чи потрібно повідомляти НОЗД?	
Дата публічного повідомлення	
Ім'я особи, яка повідомляє	
Чи потрібно інформувати зацікавлені сторони?	
Дата інформування зацікавлених сторін	
Дата реєстрації (рік, місяць, день)	

Положення про введення в дію:
Ці Правила набувають чинності 30 серпня 2024 року.
Підписано та затверджено Генеральним директором 30 серпня 2024 року.

Видача документа

Підготовлено Адвокатським бюро доктора Фрідмана Роберта

EWG Customs Agency Zrt.
1134 Budapest,
Róbert Károly krt. 59.
Adószám: 24438635-2-41
Cgjsz: 01-10-141551

EWG Customs Agency Ltd.: в особі Еріки Полц, генерального директора