NEEKA
E-mail: info@neeka.org

Міжнародний фонд охорони здоров'я та навколишнього середовища "Регіон Карпат"

INTERNATIONAL FOUNDATION FOR HEALTH AND ENVIRONMENT PROTECTION „ REGION KARPAT"

Україна, 89600 м.Мукачево, вул. Мічуріна 3
тел./факс: +38 (03131) 32122, 31450

Ukraine, 89600, Mukachevo, st.Michurina,3
tel./fax: +38 (03131) 32122, 31450

Затверджено

директором МФОЗНС «РЕГІОН КАРПАТ» NEEKA

Пірчак А. І.

Політика захисту персональних даних

1. Загальні положення

Політика захисту персональних даних – правила, якими регламентується процедура безпеки, збереження, передачі персональних даних, що можуть бути запитані/отримані при здійснені завдань та цілей МФОЗНС "РЕГІОН КАРПАТ" далі (Організація) .

Персональні дані – відомості чи сукупність відомостей про фізичну або юридичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Дана політика була розроблена на основі Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних», Політики УВКБ ООН «щодо захисту персональних даних підмандатних осіб» та ЗУ «Про захист персональних даних»

2. Принципи опрацювання персональних даних

Персональні дані необхідно:

(а) опрацьовувати у законний, правомірний і прозорий спосіб щодо суб'єкта даних («законність, правомірність і прозорість»);

(б) збирати для визначених, чітких і законних цілей і в подальшому не опрацьовувати у спосіб, що є несумісним з такими цілями;

(в) вважати достатніми і відповідними та обмежити їх мірою необхідності в них з огляду на цілі опрацювання («мінімізація даних»);

(г) вважати точними і, за необхідності, оновлювати; необхідно вживати усіх відповідних заходів для того, щоб забезпечити, що неточні персональні дані, зважаючи на цілі їхнього опрацювання, було стерто чи виправлено без затримки («точність»);

(ґ) зберігати в формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їхнього опрацювання; персональні дані можна зберігати протягом більш тривалих періодів, доки їх опрацьовують виняткова для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей за умов вжиття відповідних технічних і організаційних заходів («обмеження зберігання»);

(д) опрацьовувати в спосіб, що забезпечує належну безпеку персональних даних, у тому числі, захист проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання шкоди, із застосуванням відповідних технічних і організаційних інструментів («цілісність і конфіденційність»).

3. Характер і мета обробки

(а) Збір персональних даних для надання правової та соціальної допомоги суб'єкту даних, з огляду на їх обмежений доступ до належних правових послуг та допомоги або відсутність окремих форм допомоги з боку державних виконавців;

(б) Збір реєстраційних даних, необхідних для підтримки та забезпечення постійного процесу реєстрації з використанням бази даних УВКБ ООН proGres v4;

(в) Різні типи направлень фізичних осіб, в тому числі до Державної міграційної служби та центрів безоплатної правової допомоги (БПД), державних центрів зайнятості або соціальних центрів; органи по догляду за дітьми.

(г) Організація також збирає Персональні дані після встановлення факту народження згідно з рішеннями суду та встановлення особи, звернення до консульських установ, під час судової процедури щодо тримання під вартою, видворення, соціальної та медичної допомоги суб'єктам даних.

Спеціалізована діяльність: засоби до існування
(а) Ідентифікувати осіб та/або домогосподарства для надання підтримки засобів до існування
(б) Надавати підготовчі програми/тренінги суб'єктам даних для підтримки засобів до існування
(в) Забезпечити навчання професійним / технічним навичкам / життєвим навичкам
(г) Проведення базового/кінцевого моніторингу підтримки засобів до існування

4. Елементи персональних даних, необхідні для обробки

4.1. З огляду на спеціалізовану діяльність та для конкретної та обмеженої мети, Організація оброблятиме наступні елементи персональних даних:

- Біометричні дані
- Деталі реєстрації
- Дані щодо засудження до кримінальної відповідальності
- Дані про стан здоров'я, статеве життя
- Адреси та контактні дані
- Документи про освіту
- Дані про навички та досвід роботи
- Інтерв'ю та додаткова інформація про реєстрацію

Порядок збору, оновлення та обробки відповідних елементів даних, зібраних та зафіксованих , визначений у цій Політиці

4.2 В рамках спеціалізованої діяльності та для конкретної та обмеженої мети. Організація оброблятиме елементи даних, які описані в розділі 4.1 під час початкових та безперервних реєстраційних дій.

5. Інформація та доступ до персональних даних

5.1. Якщо персональні дані щодо суб'єкта даних збирають від суб'єкта даних, Організація повинна, у момент отримання персональних даних, надати суб'єкту даних усю інформацію, а саме інформацію про:

(а) особу та контактні дані Організації та, за необхідності, представника Організації;

(б) контактні дані співробітника з питань захисту даних, за необхідності;

(в) цілі опрацювання, для досягнення яких призначено персональні дані, а також законодавчу базу для опрацювання;

(г) одержувачі чи категорії одержувачів персональних даних, за наявності;

(ґ) за необхідності, інформацію про те, що Організація має намір передати персональні дані до третьої країни чи міжнародної організації.

5.2. Крім інформації, вказаної в пункті 5.1., Організація повинна, у момент отримання персональних даних, надати суб'єкту даних усю детальну інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, а саме інформацію про:

(а) період зберігання персональних даних, або, якщо це неможливо, - критерії визначення такого періоду;

(б) існування права на запит від Організації щодо доступу до персональних даних і їх виправлення, стирання, обмеження опрацювання щодо суб'єкта даних або на заперечення проти опрацювання, а також права на мобільність даних;

(г) право подавати скаргу до наглядового органу;

(ґ) те, чи є надання персональних даних статутною чи договірною вимогою, або вимогою, необхідною для укладення контракту, а також - чи зобов'язаний суб'єкт даних надати персональні дані, та про можливі наслідки ненадання таких даних;

5.3. Якщо Організація прагне надалі опрацьовувати персональні дані для іншої цілі, ніж та, для якої персональні дані було отримано, Організація повинна надати суб'єкту даних до початку такого подальшого опрацювання інформацію про таку іншу ціль і будь-яку належну детальну інформацію.

5.4. Відстрочення або відмова у доступі до персональних даних

Відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.

Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.

Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

6. Зберігання та передача персональних даних

6.1 Організація зберігатиме фізичні файли персональних даних у захищених картотеках, захищених від подачі документів у приміщенні Організації. Фізичні файли персональних даних повинні бути захищені розумними та належними заходами від несанкціонованої зміни, підробки, незаконного знищення, випадкової втрати, неналежного розголошення або неправомірної передачі.

6.2. Організація буде зберігати електронні файли персональних даних на захищеному сервері.

6.3. Будь-яке передавання персональних даних, що перебувають в процесі опрацювання чи призначені для опрацювання після передавання до третьої країни чи міжнародної організації, повинне відбуватися лише у разі, якщо з урахуванням інших положень цієї політики Організація дотримується всіх умов, в тому числі, для наступних актів передавання персональних даних з третьої країни чи міжнародної організації до іншої третьої країни чи міжнародної організації.

6.4. Передавання персональних даних до третьої країни чи міжнародної організації може відбуватися, якщо Організація вирішила, що третя країна, територія чи один або декілька визначених секторів у межах такої третьої країни, або відповідна міжнародна організація, забезпечує належний рівень захисту. Таке передавання не вимагає отримання будь-якого спеціального дозволу.

7. Права суб'єктів даних

7.1. Право суб'єкта даних на доступ

Суб'єкт даних повинен мати право на отримання від Організації підтвердження факту опрацювання її або його персональних даних і, якщо це так, - доступ до персональних даних та інформації про:

(а) цілі Організації;

(б) категорії відповідних персональних даних;

(в) одержувачі чи категорії одержувача, якому персональні дані були або будуть розкриті, зокрема, одержувачі в третіх країнах або міжнародній організації;

(г) за можливості, період, протягом якого передбачається, що персональні дані будуть зберігати, або, якщо це неможливо, - критерії визначення такого періоду;

(ґ) існування права надсилати запит до Організації щодо виправлення чи стирання персональних даних, або обмеження опрацювання персональних даних про суб'єкта даних і заперечувати проти такого опрацювання;

(д) право подавати скаргу до наглядового органу;

Якщо персональні дані передають до третьої країни або до міжнародної організації, суб'єкт даних повинен мати право бути повідомленим про належні гарантії.

Організація повинна надати копію персональних даних, які знаходяться у процесі опрацювання. Для будь-яких подальших копій, запит на які надсилатиме суб'єкт даних, Організація може стягувати розумну плату, що ґрунтується на адміністративних витратах. У разі подання суб'єктом даних запиту електронними засобами і за винятком його прохання щодо іншої форми інформацію необхідно надавати загальноприйнятими електронними засобами.

Право на отримання копії, не повинно негативно впливати на права та свободи інших осіб.

7.2. Право на виправлення

Суб'єкт даних повинен мати право на виправлення його або її неточних персональних даних, яке повинна здійснити Організація без будь-якої необґрунтованої затримки. Зважаючи на цілі опрацювання, суб'єкт даних повинен мати право заповнити незаповнені персональні дані, в тому числі, надавши додаткову заяву.

7.3. Право на стирання («право бути забутим»)

Суб'єкт даних повинен мати право на стирання своїх персональних даних, яке повинна здійснити Організація без будь-якої безпідставної затримки, також Організація повинна бути зобов'язана стерти персональні дані без будь-якої необґрунтованої затримки у разі виникнення однієї з наведених нижче підстав:

(а) немає більше потреби в персональних даних для цілей, для яких їх збирали чи іншим чином опрацьовували;

(б) персональні дані опрацьовували незаконно;

(в) персональні дані необхідно стерти для дотримання встановленого законом зобов'язання, закріпленого в законодавстві, яке поширюється на Організацію;

(г) персональні дані збирали в зв'язку з пропонуванням послуг інформаційного суспільства.

7.4. Право на обмеження опрацювання

Суб'єкт даних повинен мати право на обмеження опрацювання Організацією у разі настання таких обставин:

(а) точність персональних даних оскаржує суб'єкт даних, протягом періоду часу, що надає Організації можливість перевірити точність персональних даних;

(б) опрацювання є незаконним та суб'єкт даних виступає проти стирання персональних даних і натомість надсилає запит на обмеження їх використання;

(в) Організації більше не потрібні персональні дані для цілей опрацювання, але їх вимагає суб'єкт даних для формування, здійснення або захисту правових претензій;

(г) суб'єкт даних заперечив проти опрацювання в очікуванні проведення перевірки щодо того, чи переважають законні підстави Організації над законними інтересами суб'єкта даних.

Якщо опрацювання було обмежено відповідно, такі персональні дані необхідно, за винятком зберігання, опрацьовувати лише за згоди суб'єкта даних або для подання, реалізації або захисту правових претензій або для захисту прав іншої фізичної або юридичної особи чи на підставах важливого суспільного інтересу.

Організація повинна повідомити суб'єкта даних, який домігся обмеження опрацювання згідно, до моменту скасування обмеження на опрацювання.

7.5. Зобов'язання щодо повідомлення про виправлення чи стирання персональних даних або обмеження опрацювання

Організація повинна повідомити про будь-яке виправлення чи стирання персональних даних або обмеження опрацювання, кожного одержувача, якому було розкрито персональні дані, за винятком, якщо це неможливо або викликає несумісні наслідки. Організація повинна повідомити суб'єкта даних про таких одержувачів, якщо суб'єкт даних надсилає про це запит.

8. Захист та безпека даних

8.1. Зважаючи на сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяг, контекст і цілі опрацювання, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які може спричинити опрацювання, Організація повинна, у момент визначення засобів опрацювання та в момент власне опрацювання, вжити необхідних технічних і організаційних заходів, таких як використання псевдонімів, призначених для результативної реалізації принципів захисту даних, зокрема, мінімізації даних, і включення необхідних гарантій до опрацювання для досягнення відповідності вимогам цієї Політики та забезпечення захисту прав суб'єктів даних.

8.2. Організація повинна вжити відповідних технічних і організаційних заходів для гарантування того, що за замовчуванням опрацьовують лише ті персональні дані, які є необхідними для кожної спеціальної цілі опрацювання. Такий обов'язок застосовують до кількості зібраних персональних даних, ступеня їхнього опрацювання, періоду їхнього зберігання та їхньої доступності. Зокрема, такими заходами необхідно гарантувати ненадання за замовчуванням доступу до персональних даних без звернення особи до невизначеної кількості фізичних осіб.

8.3. Зважаючи на сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяги, контекст і цілі опрацювання, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які викликає опрацювання, Організація повинна вжити необхідних технічних і організаційних заходів для забезпечення рівня безпеки відповідно до ризику, в тому числі, між іншим, у належних випадках:

(а) використання псевдонімів і шифрування персональних даних;

(б) здатність забезпечувати безперервну конфіденційність, цілісність, наявність та стійкість систем та послуг опрацювання;

(в) здатність вчасно відновити наявність і доступ до персональних даних у випадку технічної аварії;

(г) процес для регулярного тестування, оцінювання та аналізу результативності технічних і організаційних заходів для гарантування безпеки опрацювання.

8.4. Оцінюючи належний рівень безпеки, необхідно враховувати, зокрема, ризики, пов'язані з опрацюванням, зокрема такі, що виникають внаслідок випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або іншим чином опрацьовано.

8.5. Організація повинна вжити заходів для того, щоб забезпечити, що будь-яка фізична особа, яка діє під керівництвом Організації і має доступ до персональних даних, не опрацьовує їх, за винятком, якщо вона здійснює це за інструкціями Організації, окрім випадків, коли вона зобов'язана діяти таким чином відповідно до законодавства.

9. Записи опрацювання даних

9.1. Організація і, за необхідності, представник Організації повинні вести запис опрацювання даних, що належать до їх сфери відповідальності. Такий запис повинен містити всю інформацію про:

(а) особу та контактні дані Організації та співробітника з питань захисту даних;

(б) цілі цієї Політики;

(в) опис категорій суб'єктів даних і категорій персональних даних;

(г) категорії одержувачів, яким персональні дані були або будуть розкриті, в тому числі одержувачі в третіх країнах або міжнародні організації;

(ґ) за необхідності, передавання персональних даних третій країні або міжнародній організації, в тому числі, ідентифікацію такої третьої країни чи міжнародної організації та, в разі актів передавання, документацію відповідних гарантій;

(д) за можливості, - передбачені часові обмеження для стирання різних категорій даних;

(е) за можливості, - загальний опис технічних і організаційних заходів безпеки

9.2. Записи, вказані в пункті 9.1., повинні бути оформлені в письмовій формі, в тому числі, - в електронній.

10. Повідомлення суб'єкта даних про порушення захисту персональних даних

10.1. Якщо порушення захисту персональних даних ймовірно призведе до виникнення високого ризику для прав і свобод фізичних осіб, Організація повинна повідомити суб'єкта даних про порушення захисту персональних даних без необґрунтованої затримки.

10.2. Повідомлення суб'єкта даних, описує, з використанням чітких і простих формулювань, специфіку порушення захисту персональних даних.

10.3. Повідомлення суб'єкта даних, є необов'язковим у разі виконання однієї з наведених нижче вимог:

(а) Організація вжила необхідних технічних та організаційних заходів захисту, і такі заходи було застосовано до персональних даних, на які вплинуло порушення захисту персональних даних, зокрема ті, що унеможливлюють розуміння персональних даних будь-якою особою, яка не має дозволу на доступ до них, наприклад, шифрування;

(б) Організація вжила наступних заходів, що гарантують, що високий ризик для прав і свобод суб'єктів даних, вказаний у пункті 10.1., ймовірно більше не матеріалізується;

10.4. Якщо Організація ще не повідомила суб'єкта даних про порушення захисту персональних даних, наглядовий орган, розглянувши ймовірність спричинення порушенням захисту персональних даних високого ризику, може вимагати зробити це чи може вирішити, що будь-яку з умов, вказаних в пункті 10.3, виконано.

11. Право на дієвий судовий засіб правового захисту

11.1. Без обмеження будь-якого наявного адміністративного або судового засобу правового захисту, в тому числі права на подання скарги до наглядового органу, кожний суб'єкт даних повинен мати право на дієвий судовий засіб правового захисту, якщо він вважає, що його права за цією Політикою було порушено внаслідок опрацювання його персональних даних, що не відповідає цій Політиці.

11.2. Провадження щодо Організації здійснюють в судах держави, де має осідок Організація. Крім того, таке провадження можна здійснювати в судах держави, за місцем постійного проживання суб'єкта даних.

12. Право на відшкодування та відповідальність

12.1. Будь-яка особа, що зазнала матеріальної або нематеріальної шкоди в результаті порушення цієї Політики, має право на отримання відшкодування від Організації за заподіяну шкоду.

12.2. Організація, несе відповідальність за шкоду, заподіяну опрацюванням, що порушує положення цієї Політики. Організація несе відповідальність за шкоду, заподіяну опрацюванням лише тоді, коли вона не дотримується обов'язків за цією Політикою, спрямованих безпосередньо на Організацію, або якщо вона діє поза чи всупереч законодавству.

12.3. Організація звільняється від відповідальності, якщо доведе, що жодним чином не несе відповідальності за подію, що спричиняє нанесення шкоди.

12.4. Судове провадження щодо реалізації права на отримання відшкодування здійснюють в судах, за місцем знаходження Організації.