ЗАТВЕРДЖЕНО
Постанова Президії Правління Товариства Червоного Хреста України
від «12» листопада 2024 р. №16/1

Політика
захисту даних (інформації)
у Товаристві Червоного Хреста України

І. Загальні положення

1.1. Політика захисту даних (інформації) у Товаристві Червоного Хреста України (далі − Політика) розроблена для здійснення Товариством системи заходів, що забезпечують збереження, цілісність даних (інформації) та належний порядок доступу до них у відповідності до міжнародних, європейських та національних стандартів захисту даних (інформації).

1.2. Положення Політики базуються на:

законах України «Про інформацію», «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах» та інших актах законодавства України;

Регламенті 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, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (далі − GDPR);

серії міжнародних стандартів ISO/IEC 27000, яка включає стандарти інформаційної безпеки, опубліковані спільно Міжнародною Організацією зі стандартизації (ISO) та Міжнародною електротехнічною Комісією (IEC);

стандартах NIST Cybersecurity Framework (CSF), NIST Special Publication (SP) 800-53 та інших стандартах, розроблених Національним інститутом стандартів та технологій США (NIST Cybersecurity Standards).

1.3.Метою Політики є:

1) визначення єдиних принципів і загальних засад процедур обробки даних (інформації) у Товаристві та його організаціях;

2) формування підстав для визначення єдиної системи адміністративних, організаційних, технічних та інших заходів, спрямованих на забезпечення збереження, захисту, конфіденційності, цілісності та належного порядку доступу до персональних даних фізичних осіб та інших даних (інформації), які обробляються Товариством та його організаціями;

3) забезпечення безпеки інформації, яка обробляється в інформаційних та інформаційно-комунікаційних системах Товариства (далі – інформаційні системи), документах та інших матеріальних носіях інформації;

4) захист Товариства від загроз втрати даних, витоку інформації, несанкціонованого доступу та інших ризиків інформаційною безпеки;

5) встановлення засад контролю захисту даних та інформації.

1.4. Ця Політика застосовується:

1) у Товаристві Червоного Хреста України, його обласних, Київській міській, місцевих організаціях, а також у Національному комітеті Товариства;

2) всіма волонтерами, працівниками Товариства та особами, які надають Товариству послуги за договорами цивільно-правового характеру;

3) до всіх видів даних (інформації), що обробляються у Товаристві на матеріальних носіях або в електронній формі, включаючи:

а) персональні дані;

б) дані (інформацію), що стосуються фінансової діяльності, бюджету, правочинів та інших операційних аспектів діяльності (далі − операційні та фінансові дані);

в) інформацію, яка є або може бути комерційною таємницею та/або іншою конфіденційною інформацією;

г) дані та інформацію, що зберігається та обробляється в інформаційних системах Товариства, включаючи сервери, хмарні ресурси, локальні бази даних та інші цифрові носії.

1.5. Принципи та основні положення цієї Політики застосовуються до фізичних та юридичних осіб усіх форм власності, з якими Товариство вступає або має намір вступити в господарські правовідносини, партнерів та інших осіб, які взаємодіють з Товариством.

ІІ. Засади організації захисту даних (інформації) Товариства

2.1. Реалізація будь-якою особою права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси Товариства та інших юридичних осіб.

2.2. Основним принципом обробки даних (інформації) у Товаристві є правомірність одержання, використання, поширення, зберігання та захисту інформації.

2.3. Охорона та захист даних (інформації) є одним з основних видів діяльності Товариства, спрямованого на забезпечення реалізації його статутних завдань.

2.4. За порядком доступу операційні та фінансові дані, також інша інформація, яка обробляється Товариством та його організаціями, поділяється на відкриту інформацію та конфіденційну інформацію.

2.5. Будь-яка інформація Товариства є відкритою, крім тієї, що віднесена законом та виданими відповідно до закону локальними нормативними актами Товариства до конфіденційної інформації.

2.6. Конфіденційною є інформація, яка обробляється у Товаристві та його організаціях:

1) персональні дані про фізичну особу;

2) інформація, доступ до якої обмежено фізичною особою, про що повідомлено Товариство;

3) інформація, доступ до якої обмежено Товариством або організаціями Товариства;

4) інформація, доступ до якої обмежено іншими юридичними особами, про що повідомлено Товариство;

5) інформація, визнана такою на підставі закону.

2.7. Порядок та підстави віднесення інформації, доступ до якої обмежено Товариством або організаціями Товариства, до конфіденційної інформації, а також порядок надання доступу до неї здійснюється за порядку, встановленими локальними нормативними актами Товариства.

ІІІ. Захист персональних даних

3.1. Реалізація завдань більшості статутних напрямів діяльності Товариства безпосередньо пов’язана з обробкою персональних даних бенефіціарів та інших фізичних осіб.

3.2. Обробка персональних даних у Товаристві має здійснюватися з метою, яка сформульована в законах, інших нормативно-правових актах України або в рішеннях керівних органів чи інших локальних нормативних актах Товариства та яка відповідає законодавству про захист персональних даних.

3.3. Обробка персональних даних здійснюється на підставі згоди суб’єкта персональних даних або іншої правової підстави, передбаченої Законом України «Про захист персональних даних» та GDPR.

3.4. Товариство зобов’язується надавати суб’єктам персональних даних зрозумілу та доступну інформацію про те, як їхні дані будуть використовуватися, та отримувати чітку згоду перед початком обробки.

3.5. Товариство та його організації повинні бути спроможними довести, що суб’єкт надав згоду на опрацювання своїх персональних даних шляхом добровільного волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

3.6. При обробці персональних даних Товариство безумовно та сумлінно забезпечує суб’єктам персональних даних права, надані їм Законом України «Про захист персональних даних» та GDPR.

3.7. Персональні дані у Товаристві необхідно обробляти з дотриманням вимог, встановлених Законом України «Про захист персональних даних» та принципів, визначених GDPR:

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

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

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

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

5) зберігати в формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їх обробки;

6) обробка в спосіб, що забезпечує належну безпеку персональних даних, у тому числі, захист проти несанкціонованої чи незаконної обробки та проти ненавмисної втрати, знищення чи завдання шкоди, із застосуванням відповідних технічних і організаційних інструментів («цілісність і конфіденційність»);

7) Товариство та його організації повинні бути здатними довести, що персональні дані обробляються з дотриманням вимог та принципів, визначених підпунктами 1-6 цього пункту («підзвітність»).

3.8. Персональні дані, зібрані з порушенням вимог Закону «Про захист персональних даних», підлягають видаленню або знищенню у встановленому законодавством порядку.

3.9. У разі порушення безпеки персональних даних Товариство негайно повідомляє про це відповідні органи та суб'єктів даних у встановлені законом терміни. Товариство зобов'язується вжити необхідних заходів для мінімізації наслідків порушення та запобігання його повторенню.

3.10.Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних на обробку цих даних, наданої Товариству, або відповідно до вимог закону.

IV. Захист даних та інформації в інформаційних системах

4.1. Доступ до інформаційних систем та мереж надається виключно уповноваженим особам відповідно до їхніх службових обов'язків. Товариство забезпечує належний рівень контролю доступу, включаючи впровадження ролей та дозволів, а також регулярний аудит доступу.

4.2. Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

4.3. Конфіденційна інформація, яка обробляється в інформаційних систем, повинна бути зашифрована під час передачі та зберігання, щоб запобігти несанкціонованому доступу.

Товариство використовує сучасні методи шифрування для захисту даних на всіх етапах їх обробки.

4.4. Товариство регулярно проводить аудити безпеки інформаційних систем та оцінку ризиків для виявлення та усунення вразливостей.

Аудити безпеки проводяться на регулярній основі, а також після будь-яких значних змін в інформаційних системах або в разі виникнення нових загроз.

4.5. Товариство забезпечує впровадження та підтримку технічних засобів захисту інформації, таких як брандмауери (фаєрволи), антивірусне програмне забезпечення, системи виявлення вторгнень тощо. Всі ці засоби регулярно оновлюються та налаштовуються відповідно до сучасних стандартів безпеки.

V. Захист інформації у документах

5.1. Документи, що містять про особу (персональні дані), іншу конфіденційну інформацію, повинні бути класифіковані та відповідно захищені.

Товариство впроваджує систему класифікації документів, на основі якої в залежності від виду конфіденційної інформації визначає відповідні заходи її захисту.

5.2. Для забезпечення фізичної безпеки документів та інших матеріальних носіїв інформації використовуються необхідні засоби захисту.

Документи та інші матеріальні носії інформації повинні зберігатися у захищених приміщеннях з обмеженим доступом.

5.3. Усі паперові документи, що містять конфіденційну інформацію, повинні бути належним чином знищені після закінчення строку зберігання.

5.4. Доступ до документів з конфіденційною інформацією надається лише уповноваженим особам для виконання завдань відповідно до їх посадових інструкцій.

Всі запити на доступ повинні бути задокументовані та розглянуті щодо надання доступу відповідно до процедур, встановлених локальними нормативними актами Товариства.

VI. Навчання та підвищення кваліфікації

6.1. Усі працівники, волонтери Товариства та особи, які надають Товариству послуги за договорами цивільно-правового характеру обов’язково проходять навчання з питань захисту даних (інформації) та інформаційної безпеки. Навчання проводиться регулярно, та має забезпечувати актуальність їх знань та навичок.

6.2. Програми навчання включають основи захисту даних (інформації), виявлення та запобігання загрозам безпеці, використання засобів захисту інформації, а також у разі необхідності специфічні вимоги (вимоги серії міжнародних стандартів ISO/IEC 27000, GDPR тощо).

6.3. Навчальні програми оновлюються відповідно до змін у законодавстві, технологіях та локальних нормативних актах Товариства. Особлива увага приділяється підвищенню обізнаності працівників та волонтерів про нові загрози та методи захисту інформації.

VII. Контроль за виконанням Політики

7.1. Контроль за виконанням Політики в Товаристві та організаціях Товариства здійснюється підрозділом з управління ризиками Національного комітету Товариства.

7.2. Товариство впроваджує внутрішні процедури контролю та аудиту для забезпечення відповідності Політики захисту даних.

7.3. Регулярні перевірки та аудити допомагають виявляти та усувати порушення в процесах обробки та захисту даних.

7.4. Усі інциденти, пов’язані із порушенням безпеки даних, повинні негайно розглядатися.

7.5. Відповідальні особи зобов’язані вживати необхідних заходів для розслідування інциденту, усунення наслідків та запобігання повторенню.

7.6. Особи, вині у невиконанні обов’язків щодо захисту даних (інформації) несуть відповідальність згідно із законом.

VIII. Заключні положення

8.1. Ця Політика підтримується в актуальному стані та переглядається не рідше одного разу на рік з метою вдосконалення системи захисту даних (інформації) у Товаристві Червоного Хреста, а також у разі змін у законодавстві України.

Про результати такого перегляду структурним підрозділом з управління ризиками інформується Генеральний директор Національного комітету Товариства.

8.2. За потреби зміни до цієї Політики можуть оформлюватися шляхом внесення окремих змін або шляхом викладення Політики в новій редакції.

8.3. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, зокрема у зв’язку з прийняттям нових нормативно-правових актів, Політика діє лише в тій частині, яка не суперечить чинному законодавству України.

_____