

ВЪТРЕШНИ ПРАВИЛА

на Институт за изследвания на мира - Пловдив за мерките за защита на личните данни съгласно Регламент 2016/679

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Институт за изследвания на мира - Пловдив, наричана по-долу само „ИИМП“ е юридическо лице с нестопанска цел, регистрирано в обществено-полезна дейност, основано, за да развива и утвърждава мира и духовните ценности, образованието, науката, културата и гражданското общество с фокус върху овластяването на момичета и жени и да популяризира и подпомага ролята на жените по въпросите на мира и сигурността е регистрирано по Закона за регистър Булстат 177006327

(2) ИИМП е със седалище в гр. Пловдив и адрес на управление: гр. Пловдив, ул. Чорлу 57

(3) ИИМП обработва лични данни във връзка със своята дейност и сама определя целите и средствата за обработването им. В този случай ИИМП действа като администратор на лични данни.

(4) В случаите, в които ИИМП обработва лични данни за цели, определени самостоятелно от трето лице или целите са определени съвместно от ИИМП и трето лице, ИИМП има положението или на обработващ лични данни (ако целите са определени от лицето, което е възложило обработването) или на съадминистратор.

Чл. 2. Настоящите Вътрешни правила на ИИМП уреждат организацията на обработване и защитата на лични данни при осъществяването дейността на организацията.

Чл. 3. (1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) „Обработване на лични данни“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез

предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбинирание, ограничаване, изтриване или унищожаване.

(3) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

Чл. 4. (1) ИИМП е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.

(2) Като администратор на лични данни, при обработването на лични данни ИИМП спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

Чл. 5. (1) Принципите за защита на личните данни са:

1. **Законосъобразност, добросъвестност и прозрачност** - обработване при наличие на законово основание, при полагане на дължимата грижа и при информирание на субекта на данни;
2. **Ограничение на целите** – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;
3. **Свеждане на данните до минимум** – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;
4. **Точност** – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;
5. **Ограничение на съхранението** – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;
6. **Цялостност и поверителност** – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;
7. **Отчетност** – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(2) Ако конкретната цел или цели, за които се обработват лични данни от ИИМП, не изискват или вече не изискват идентифициране на субекта на данните, ИИМП не е задължена да поддържа, да се слобие или да обработи допълнителна информация за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

Чл. 6. ИИМП организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. ИИМП прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;

Чл. 8. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на ИИМП и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на ИИМП се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 9. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от ИИМП, подписват декларация за съгласие по образец (*Приложение № 1*).

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само органите на ИИМП, съобразно възложените им от закона правомощия и оторизираните работници и служители на ИИМП, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните.

(2) Оторизирането на работници и служители се извършва на база длъжностна характеристика или чрез изричен акт на Председателя на ИИМП

(3) Работниците и служители носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните работници и служители.

(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Чл. 11. (1) Документите и преписките, по които работата е приключила, се архивират.

Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство.

(2) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият/операторът/ на лични данни и оторизираните длъжностни лица.

(3) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица и органите на ИИМП съобразно възложените им от закона правомощия.

Чл. 12. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

Чл. 13. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, ИИМП може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години или при промяна на характера на обработваните лични данни.

Чл. 14. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от ИИМП регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, ИИМП прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(3) Унищожаване се осъществява от служители, упълномощени с изричен писмен акт на Председателя на ИИМП и след уведомяване на Длъжностното лице по защита на данните

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 3, съгласно образец, представляващ **Приложение № 2**.

Чл. 15. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство.

(2) Третите страни получават достъп до лични данни, обработвани в ИИМП, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ, Висш адвокатски съвет, Национално бюро за правна помощ и др.п.).

II. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 16. Физическата защита в ИИМП се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

(1) Документите, съдържащи лични данни, се съхраняват в *шкафове или картотеки, които могат да се заключават*. Ключ за шкафите притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).

Чл. 17. (1). Основните *мерки за персонална защита* на личните данни, приложими в ИИМП, са:

1. Задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминаването обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни по образец (*Приложение № 3*);
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от ИИМП;
3. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

(2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен мерките по ал. 1 и следните допълнителни мерки::

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

Чл. 18. (1). Основните *мерки за документална защита* на личните данни, са:

1. *Определяне на регистрите, които ще се поддържат на хартиен носител* - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на ИИМП, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;
2. *Определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на ИИМП, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;
3. *Регламентиране на достъпа до регистрите с лични данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае“;
4. *Определяне на срокове за съхранение* - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.

5. *Процедури за унищожаване:* Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на ИИМП или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(2) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 1, се прилагат и следните допълнителни мерки:

1. *Контрол на достъпа до регистрите*, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае”, за да изпълняват техните задължения;
2. *Правила за размножаване и разпространение*, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

III. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 19. (1) Длъжностно лице по защита на данните се определя от Ръководството на ИИМП.

(2) Длъжностно лице по защита на данните има следните правомощия и длъжностни задължения:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри с лични данни;
3. осъществява контрол по спазване на изискванията за защита на регистрите съобразно действащото законодателство и настоящите вътрешни правила;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;

7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрацията на всички извършени действия с регистрите в компютърната среда;
8. определя ред за съхраняване и унищожаване на информационни носители;
9. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;
10. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, за целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;
11. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

Чл. 20. Служителите на ИИМП са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират при необходимост регистрите на личните данни;
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

Чл. 21. (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за ИИМП или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

VI. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 22. Всички служители на ИИМП са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

Чл. 23. (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни,.

(2) Приложение към настоящите Вътрешни правила са образци на следните документи, съставяни при и по повод обработката на лични данни:

- **Приложение № 1** – *Декларация-съгласие за обработка на лични данни* (която се подписва, когато обработването не се извършва на друго основание, предвидено в чл. 6 от Регламент 2016/679);

- **Приложение № 2** – образец на Протокол за унищожаване на лични данни и носители на лични данни.

- **Приложение № 3** - Протокол за преминато обучение по защита на личните данни и инструктаж за приложимите правила и мерки за защита на личните данни;