Утвърдил:

29.10.2020 г.

X

Владимир Бояджиев
Директор
Signed by: Vladimir Georgiev Boyadjiev

Вътрешни правила за защита на личните данни в Националния институт за помирение и арбитраж

София, октомври 2020 г.

1618 София, ж.к. „Овча купел”, ул. „Боряна” №59, бл.215А, ет.1, ап.1
тел.: 02/425 3750; факс: 02/425 3760; E-mail: nipa@nipa.bg; Web: www.nipa.bg

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Националният институт за помирение и арбитраж, наричан по-долу само НИПА е юридическо лице към министъра на труда и социалната политика и е регистриран по Закона за регистър БУЛСТАТ с БУЛСТАТ: 131083803.

(2) НИПА е със седалище в гр. София и адрес на управление: гр. София, ул. „Боряна“ № 59, бл.215А, ет.1, ап.1.

(3) Като юридическо лице, възникнало по силата на закона, НИПА осъществява чрез своите органи дейностите, предвидени в Закона за уреждане на колективните трудови спорове и Правилника за устройството и дейността на НИПА.

(4) НИПА обработва лични данни във връзка със своята дейност и определя целите и средствата за обработването им, поради което има качеството на администратор на лични данни

(5) В качеството си на публична администрация НИПА определя длъжностно лице по защита на личните данни. Данните за контакт с длъжностното лице по защита на данните се обявяват на лесно достъпно място на официалната интернет страница, както и в утвърдената Политика за поверителност на личните данни.

Чл. 2. Настоящите Вътрешни правила за защита на личните данни (наричани за краткост „Вътрешни правила“) уреждат организацията на обработване и защитата на лични данни на посредниците и арбитрите, които са включени в Списъците на посредници и арбитри към НИПА, на членовете на Надзорния съвет към НИПА, на работниците/служителите, включително и на кандидатите за работа в НИПА, на контрагентите на НИПА, както и на всички други физически лица, с които НИПА влиза в отношения при осъществяването на правомощията и дейността си.

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 комбиниране, ограничаване, изтриване или унищожаване.

(3) „Обработващ лични данни“ е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора и е лице, различно от администратора.

(4) „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.

(5) „Предоставяне на лични данни“ са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.

(6) „Псевдонимизация“ е обработване на лични данни по такъв начин, че личните данни не могат повече да бъдат свързани с конкретен субект на данни, без да се използва допълнителна информация, при условие, че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано.

(7) „Анонимизиране“ е процес, в резултат на който се създава информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран.

Чл. 4. (1) НИПА 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 НИПА 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 информиране 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 НИПА, не изискват или вече не изискват идентифициране на субекта на данните, НИПА не е задължена да поддържа, да се сдобие 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. (1) Достъпът до лични данни в НИПА се осъществява при прилагане на принципа „ограничение на целите“, регламентиран в чл.5, т.1, буква „б“ от Регламент (ЕС) 2016/679.

(2) Право на достъп до носителите на лични данни имат само лицата, които:

1. обработват данни в изпълнение на служебните си задължения, съгласно трудово правоотношение и длъжностната характеристика за съответната длъжност;
2. са оправомощени чрез изричен акт на директора на института;
3. изпълняват договори, по които НИПА е страна.

(3) Достъп до личните данни се предоставя след запознаване с нормативната уредба в областта на защитата на личните данни, настоящите правила и процедури за защита на личните данни на администратора.

(4) Лицата с право на достъп лица подписват Декларация за конфиденциалност при обработката на лични данни (***Приложение № 1.1.*** и ***Приложение № 1.2***), до които получават достъп при и по повод изпълнение на задълженията си.

(5) Лицата, които имат достъп до лични данни носят отговорност за опазване на носителите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни може да бъде основание за налагане на дисциплинарна, административна или наказателна отговорност, в предвидените от съответната нормативна уредба случаи.

Чл. 7. НИПА 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. 8. НИПА прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и мрежи;
5. Криптографска защита.

Чл. 9. (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 и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на НИПА и/или нормалното му функциониране.

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

Чл. 10. За изпълнение на задължението на НИПА за наличие на съгласие по смисъла на чл.4, т.11 от Регламент (ЕС) 2016/679, на субектите на данни се предоставя Декларация за съгласие по образец (***Приложение № 2***).

Чл. 11. (1) НИПА съхранява лични данни на хартиен и/или електронен носител, само за времето, необходимо за изпълнение на дейностите за обработката или когато в нормативен документ е определен друг период за тяхното съхранение.

(2) Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив и за срокове, съобразени с действащото законодателство. Помещенията, определени за архив, са оборудвани със специални метални шкафове и задължително се заключват.

(3) 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 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 лични данни и оправомощените длъжностни лица.

(4) Достъп до архивираните документи, съдържащи лични данни, имат единствено оправомощените лица и ръководните органи на НИПА, 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 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, НИПА 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 НИПА регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) Правилата за съхранение, включително срокът за съхранение , както и правилата за унищожаване, когато такива не са определени в нормативната уредба или в Номенклатурата на делата със срокове за съхраняване, се определят с Процедура за съхранение и унищожаване на лични данни (***Приложение № 3***).

Чл. 15. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, НИПА съобщава в 1-месечен срок от подаване на заявлението, респ. искането.

(3) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(4) Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни по образец, съгласно (***Приложение № 4)***, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

(5) Третите страни получават достъп до лични данни, обработвани в НИПА, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ и др.п.).

II. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 16. ***Физическата защита*** в НИПА 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.

Чл. 17. (1). Основните ***организационни мерки за физическа защита*** в НИПА включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни,
3. определяне на организацията на физическия достъп;

(2) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни.

(3) *Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове*, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Лицата, които поддържат системите нямат достъп до съхраняваните в електронен вид данни.

(4) *Организацията на физическия достъп до помещения*, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(5) *Използваните технически средства за физическа защита* на личните данни в НИПА са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп с оглед изпълнението на работните им задължения.

(6) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са в кабинети с ограничен достъп само за упълномощен персонал.

Чл. 18. (1). Основните ***технически мерки за физическа защита*** в НИПА включват:

1. използване на сигнално-охранителна техника;
2. използване на ключалки и заключващи механизми;
3. шкафове, метални каси;
4. оборудване на помещенията с пожарогасителни средства.

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

(3) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва: сигнално-охранителна техника, *ключалки* (механични или електронни) за ограничаване на достъпа, заключващи шкафове и пожарогасителни средства.

(4) П*ожарогасителните средства* се разполагат в съответствие с изискванията на приложимата нормативна уредба.

Чл. 19. (1). Основните ***мерки за персонална защита*** на личните данни, приложими в НИПА, са:

1. Задължение на служителите да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като за проведения инструктаж с правилата за защита на личните данни се подписва протокол за извършен инструктаж по образец (***Приложение № 5***);

2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от НИПА;

3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..) между персонала и всякакви други лица, които са неоторизирани;

4. 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 провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно.

Чл. 20. (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 документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на основната дейност на НИПА, 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 основната дейност на НИПА, 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 оправомощените служители;

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 НИПА 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, 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 изготвяне на документи, 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.

Чл. 21. (1) ***Защитата на автоматизираните информационни системи и/или мрежи*** в НИПА включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. *Идентификация и автентификация* чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на НИПА. Прилагането на тази мярка е с цел да се регламентират нива на достъп;
2. *Управление на регистрите*, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;
3. Управление на *външни връзки и/или свързване*, включващо от своя страна:

– Дефиниране на обхвата на вътрешните мрежи: Като *вътрешни мрежи* се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на НИПА. Като *външни мрежи* се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на НИПА.

– Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени от директора на НИПА лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения. Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

– Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администриране на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на администратора.

– Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на НИПА, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4. *Защитата от зловреден софтуер* включва:

– използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от системния администратор. Забранено е инсталирането на софтуерни продукти без изричното одобрение на системния администратор.

– използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от системния администратор. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

– активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

– забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми системния администратор и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политика по *създаване и поддържане на резервни копия за възстановяване,* която регламентира:

– Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на НИПА.

– Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

– Отговорност за архивиране има лицето, обработващо личните данни.

– Срокът на архивиране следва да е съобразен с действащото законодателство.

– Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

6. Основни *електронни носители на информация са*: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети и други носители на информация, еднократно записваеми носители и др.)

7. *Персоналната защита на данните* е част от цялостната охрана на НИПА.

8. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на НИПА.

9. Данните, които вече не са необходими за целите на обработването и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

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

1. *Организация на телекомуникационните връзки и отдалечения достъп* до вътрешните мрежи на НИПА:

– Отдалечен достъп до вътрешни мрежи на НИПА е предвиден при извънредни (форсмажорни обстоятелства) и по изключение. След изричната оторизация от директора на НИПА, може да се разреши подобен достъп на определени служители, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обмена на данни.

– На персонала на НИПА може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на заместник-директора, съгласувано с директора на НИПА за лицата, за степента на осъществимост, за пряката връзка с изпълняваните задължения и свързаните с този достъп рискове. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на ръководството на НИПА, както и в случаите на заплаха за сигурността на данните.

2. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на НИПА, включват:

– Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на НИПА от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

– Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на НИПА, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако нарушението е не само дисциплинарно или

представлява престъпление – и по предвидения за санкциониране на това нарушение (престъпление) ред.

3. Мерките, свързани със създаване на *физическа среда (обкръжение),* включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Чл. 22. (1) По отношение на личните данни се прилагат и мерки, свързани с ***криптографска защита на данните*** чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване.

(2) Криптирането се използва и за защита на личните данни, които се предават от НИПА по електронен път или на преносими носители.

III. БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 23. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) НИПА прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 60 сек.), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от НИПА период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(6) Системите, обработващи и/или съхраняващи лични данни, включват система за контрол, регистрираща следните действия в журнал (log) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (например влизане в нетипично време, не

изключване на работна станция след изтичане на работното време и др.), системният администратор незабавно уведомява ръководството и длъжностното лице по защита на данните за извършване на проверка по случая.

Чл. 24. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 25. (1) В НИПА се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от системния администратор. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 26. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

IV. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 27. Поддържаните от НИПА регистри с лични данни са:

1. Регистър на *„**Посредници** и **Арбитри**”;*
2. Регистър *„**Човешки ресурси, работна заплата и възнаграждения**”.*

Чл. 28. (1) Регистърът на дейностите по обработка на данни, извършвани от НИПА, в качеството на администратор на лични данни, е със следното минимално съдържание:

1. целите на обработването на лични данни;
2. категориите получатели, пред които са или ще бъдат разкрити личните данни;
3. описание на категориите субекти на данни и на категориите лични данни;
4. правното основание за операцията по обработване,
5. когато е възможно, предвидените срокове за изтриване на различните категории лични данни;
6. когато е възможно, общо описание на техническите и организационните мерки за сигурност по чл.66 от ЗЗЛД;

(2) Съответните регистри се създават и поддържат от служителите, ангажирани с дейности по обработка на личните данни.

(3) При поискване длъжностното лице по защита на личните данни предоставя достъп до тях на комисията за защита на личните данни.

(4) Регистрите на дейностите по обработка се поддържат в електронна и/или писмена форма.

V. РЕГИСТЪР НА „ПОСРЕДНИЦИ И АРБИТРИ“

Чл. 29. (1) Регистърът се поддържа от техническия сътрудник и се води на основание чл. 8, т.5, б. “д“ от Правилника за устройството и дейността на НИПА.

(2) В регистъра се вписват следните лични данни:

–*Физическа идентичност:* имена, адрес, ЕГН, телефон, електронен адрес, снимка;

–*Социална идентичност:* информация за образование - вид и степен, специалност, професионална квалификация, научни степени и звания, за владеене на чужди езици, трудова дейност – месторабота, длъжност, трудов стаж и др.;

–*Икономическа идентичност:* информация за принадлежността към организацията или държавния орган, от които са определени.

(3) Поддържането на Регистъра се осъществява на електронен носител, посредством създадена база от лични данни в персоналния компютър на обработващия данните.

(4) Данни от регистъра могат да бъдат предоставяни на лица и държавни органи с оглед изпълнение на нормативно задължение.

(5) Данни от регистъра, включваща информация за посредниците и арбитрите, свързана с тяхната професионална квалификация и опит, вкл. при решаване на колективни трудови спорове се публикува на интернет страницата на НИПА, след дадено съгласие от посредниците и арбитрите.

VI. РЕГИСТЪР „ЧОВЕШКИ РЕСУРСИ, РАБОТНА ЗАПЛАТА И ВЪЗНАГРАЖДЕНИЯ”

Чл. 30. (1) Регистърът се поддържа от главния юрисконсулт и счетоводителя в НИПА и съдържа лични данни, необходими за водене на трудови досиета, изплащане на възнаграждения и сключване и изпълнение на договори, по които физическото или юридическото лице, за което се отнасят данните е страна. Данните се събират от физическото лице, а за управители на фирми - и от публични регистри.

(2) В Регистъра се обработват следните лични данни:

- *Физическа идентичност:* име, адрес, ЕГН, паспортни данни, месторождение, телефон;
- *Семейна идентичност* - семейно положение, родствени връзки;
- *Социална идентичност* - образование, трудова дейност;
- *Осигурителен статус*;
- *Имуществено състояние*;
- *Лични данни, отнасящи се до здравето*;

- *Възнаграждения,* въз основа на ведомостите на НИПА, съхранявани в архива на НИПА– за издаване форма УП-2.

(3) Поддържането на Регистъра се осъществява на хартиен и електронен носител.

(4) Регистърът се поддържа на основание Кодекса на труда, Закон за задълженията и договорите, Кодекса за социално осигуряване (КСО), Търговския закон и др. и се отнася до персонал (по ТПО, по граждански договори), членове на Надзорен съвет на НИПА, изпълнители, извършвали услуги по договор, бивши служители.

(5) Обработващите лични данни са длъжни да не разкриват лични данни, да спазват конфиденциалност и да предприемат мерки за ограничаване достъпа до данните.

(6) Личните данни в този Регистър са на електронен носител и се съхраняват в счетоводството чрез специализиран софтуер.

(7) Личните данни от този Регистър могат да бъдат разкривани само на физическите и юридическите лица, за които се отнасят и на лицата, за които е предвидено в нормативен акт.

VII. ОЦЕНКА НА РИСКА И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЛИЧНИТЕ ДАННИ

Чл. 31. (1) НИПА извършва оценка на риска за извършваните дейности по обработване на лични данни.

(2) На базата на извършената оценка на риска се изготвя План за управление на риска, който съдържа необходимите механизми за контрол, отговорните лица и сроковете за изпълнение.

Чл. 32. НИПА извършва оценка на въздействието, когато обработката на данни създава висок риск за правата и свободите на физическите лица. Оценката на въздействието се извършва, съгласно Процедура за извършване на оценка на въздействието върху личните данни и Методология за извършване на оценка на въздействието (***Приложение № 6***).

VIII. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 33. (1) Длъжностно лице по защита на данните се определя от директора на НИПА.

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

1. информира и съветва директора за задълженията, свързани с обработването на личните данни, съгласно законодателството в областта на защита на данните и настоящите Вътрешни правила;
2. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
3. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри с лични данни;

4. осъществява контрол по спазване на изискванията за защита на регистрите, съобразно действащото законодателство и настоящите вътрешни правила;

5. 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;

6. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

7. специфицира техническите ресурси, прилагани за обработка на личните данни;

8. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите в компютърната среда;

9. определя ред за съхраняване и унищожаване на информационни носители;

10. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;

11. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;

12. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

Чл. 34. Служителите на НИПА 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. 35. (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 НИПА или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

IX. ПРАВА НА ФИЗИЧЕСКИТЕ ЛИЦА

Чл. 36. (1) Физическите лица, чиито данни се обработват от НИПА имат следните права:

1. право на достъп до данните, право на коригиране;

2. право на изтриване/право „да бъдеш забравен“;

3. право на ограничаване на обработването;
4. право на възражение;
5. право да не бъде обект на автоматизирано вземане на индивидуални решения, включително профилиране;
6. право на преносимост на данните;
7. право на жалба до надзорния орган, което е субективно право на всяко физическо лице.

(2) Всяко физическо лице, чиито лични данни се обработват от администратора, има право на информация, съгласно чл.13 и чл.14 от Общия регламент за защита на личните данни. НИПА уведомява лицата за обработката на личните данни чрез публикуване на Политика за поверителност.

(3) Уведомяване по смисъла на предходната алинея не се извършва, когато:

1. обработването е за статистически цели и предоставянето на информацията е невъзможно или изисква прекомерни усилия;
2. физическото лице, за което се отнасят данните вече разполага с информацията;
3. обработката е предвидена в закон;
4. е налице изрична нормативна забрана.

(4) Условията и реда за упражняване правата на субекта на данни, с изключение на правото на жалба до надзорния орган се съдържат в Процедура за упражняване на права от субектите на данни (***Приложение № 7***).

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила се приемат на основание чл.24, параграф 2 от регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО.

§ 2. 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, Закона за защита на личните данни и действащото приложимо законодателство, което регламентира обработката на лични данни.

§ 3. Правилата влизат в сила от датата на утвърждаването им от директора на НИПА.