

Утвърдени със Заповед  
№ 136-1-РД-19/28.05.2018г.

**ПРАВИЛА ОТНОСНО МЕХАНИЗМА НА ОБРАБОТВАНЕ И  
ЗАЩИТА НА ЛИЧНИ ДАННИ В НАЦИОНАЛЕН МУЗЕЙ  
„ЗЕМЯТА И ХОРАТА“**

**РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ**

Чл. 1. (1) Настоящите правила се прилагат за лични данни по смисъла на Закона за защита на личните данни и Регламент /EC/ 2016/ 679 (General Data Protection Regulation) на Европейския съюз.

(2) НАЦИОНАЛЕН МУЗЕЙ "ЗЕМЯТА И ХОРАТА"/НМ „Земята и хората“/ е държавен културен институт, администратор на лични данни.

(3) Принципите, на които се основават настоящите правила са:

- събиране на лични данни на законно основание и за конкретни цели;
- предприемане на адекватни технически и организационни мерки за защита на личните данни;
- повече информация за субектите на лични данни и прозрачност на дейността на администратора на лични данни;
- намаляване на злоупотребите с лични данни чрез стриктна дисциплина.

Чл. 2. (1) НМ „Земята и хората“ обработва лични данни на законово основание и за конкретни цели:

- като законово задължение на НМ „Земята и хората“ – Кодекс на труда и подзаконови нормативни актове, Закон за закрила и развитие на културата и подзаконови нормативни актове, Закон за културното наследство и подзаконови нормативни актове, Закон за задълженията и договорите и др.

- въз основа на легитимен интерес на НМ „Земята и хората“;
- във връзка с изпълнение на договор, по който субектът на лични данни е страна или за сключването на такъв, по искане на субекта;
- в други случаи - жизненоважен интерес, задача в обществен интерес или официални правомощия.

(2) Конкретни цели за обработване на данните са:

- индивидуализация на страна по договора;
- регистрация на участник в конкурс, процедура за възлагане на обществена поръчка, търг и събитие, организирано от НМ „Земята и хората“;
- счетоводни цели;
- статистически цели;
- трудовоправни цели;
- обезпечаване на изпълнението на договор;
- изпращане на информационни съобщения;
- и др.

(3) Личните данни се обработват при следните основни принципи:

- законосъобразност, добросъвестност и прозрачност;
- ограничение на целите - за конкретни, изрично указанi и легитимни цели;
- свеждане на данните до необходимия минимум - само за



целите на обработване;

- точност-точни лични данни и в актуален вид;
- ограничаване на съхранението - във форма позволяваща идентифицирането на субекта и за период не по-дълъг за целите на обработване;
- цялостност и поверителност - подходящи технически и организационни мерки за осигуряване на сигурност на личните данни;
- отчетност – възможност на НМ „Земята и хората“ във всеки момент да докаже прилагането на тези принципи;
- НМ „Земята и хората“ не събира и не обработва лични данни, които се отнасят за следното:
  - разкриват расов или етнически произход;
  - разкриват политически, религиозни или философски убеждения;
  - генетични и биометрични данни или данни за сексуалния живот или сексуалната ориентация.

**Чл. 3.** (1) Администраторът възлага обработването на личните данни на негови служители и членове на органи и експертни комисии, функциониращи към него/обработващи/. Обработването се възлага на повече от един обработващ данните, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.

(2) Обработващите лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.

**Чл. 4.** (1) Личните данни в регистрите се набират от администратора на лични данни респективно - обработващият лични данни чрез устно интервю, чрез електронна платформа и/или на хартиен носител.

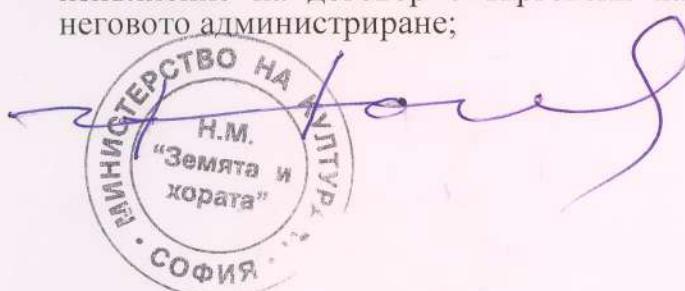
(2) За необходимостта от набиране на лични данни и целите, за които ще бъдат използвани, обработващият лични данни информира лицето.

(3) Документите, съдържащи лични данни, заедно с приложенията към тях се обработват в регистрите от обработващия лични данни.

(4) При необходимост от поправка на личните данни, лицата предоставят такива на обработващия лични данни по негово искане на основание нормативно задължение или по свое желание.

**Чл. 5.** (1) НМ „Земята и хората“ извършва следните операции с личните данни за следните цели:

1. регистрация на участник в конкурс, процедура за възлагане на обществена поръчка, търг – целта е осъществяване на законово определена процедура чрез индивидуализиране на съответното лице;
2. регистрация на лице с цел участие в събитие, организирано от НМ „Земята и хората“;
3. склучване и изпълнение на търговска сделка или договор за съвместна дейност с клиент или партньор – целта на тази операция е склучване и изпълнение на договор с търговски партньор, партньор или клиент и неговото администриране;



4. изпращане на информационни съобщения – целта на тази дейност е администриране на процеса по изпращане на съобщения до посетители и партньори.

(2) Заключение от оценката на въздействието: Въз основа на горепосочената оценка на въздействието Директорът счита, че посочените в ал. 1 операции са допустими за извършване и предоставя достатъчни гаранции за защита на правата и законните интереси на субектите на данните в съответствие с изискванията на GDPR.

**Чл. 6.** За достоверността на предоставените копия от регистри, съдържащи лични данни, отговорност носи обработващият лични данни.

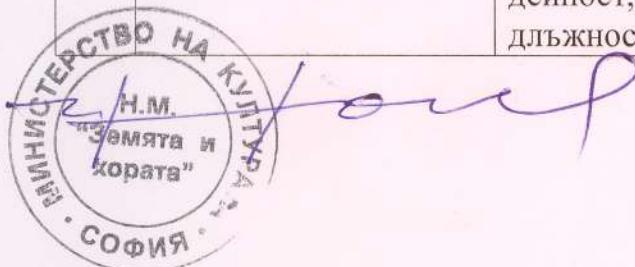
## РАЗДЕЛ II. ВИДОВЕ РЕГИСТРИ В НФК И ФОРМИ НА ВОДЕНЕТО ИМ

**Чл. 7.** В НМ „Земята и хората“ се водят и съхраняват следните официални регистри и бази данни на хартиен носител и електронна платформа:

№	Видове регистри	Видове лични данни	Служител/отдел, в които се водят регистрите
1	Картотека на личните трудови /служебни досиета на служителите в НМ „Земята и хората“	трите имена на служителя, ЕГН, адрес, данни от личната карта, местораждение, образование, трудова дейност, заемана длъжност, медицински данни, данни относно гражданско-правния статус на лицата (като свидетелство за съдимост)	Обслужващ счетоводител, Служител „Човешки ресурси“

За вътрешноведомствени цели в НФК се поддържат и съхраняват следните регистри:

1	Регистър на трудовите договори и допълнителните споразумения със служителите в НМ „Земята и хората“	трите имена на служителя, ЕГН, адрес, паспортни данни, образование, трудова дейност, заемана длъжност	Обслужващ счетоводител Служител „Човешки ресурси“
2	Дневник за издадените нови трудови книжки	трите имена на служителя, ЕГН, образование, трудова дейност, заемана длъжност	Обслужващ счетоводител Служител „Човешки ресурси“



3	Входящ регистър на обществените поръчки	имена, телефон и адрес на лицето/ имена на представляващия юридическото лице	Служителят с деловодни функции Обслужващ счетоводител
4	Регистър на договорите, сключени в НМ „Земята и хората“	имена, ЕГН и адрес на лицето	Всички служители, Обслужващ счетоводител
5.	Регистър на оферти по ЗДС и ППЗДС	имена, ЕГН и адрес на лицето	Служителят с деловодни функции

### РАЗДЕЛ III. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ

**Чл. 8.** НМ „Земята и хората“ осигурява подходящи технически и организационни мерки за обработване на личните данни съобразно нормативно установените задължения, като взетите мерки (по подразбиране) гарантират, че:

- се обработват лични данни само за конкретна цел на обработването (с оглед обем на лични данни, степен на обработване, период на съхранение и достъпност);
- до данните нямат достъп неограничен брой лица (без да е необходима допълнителна намеса от физическо лице).

**Чл. 9.** (1) Информацията, съдържаща лични данни на хартиен носител се съхранява в папки, които се подреждат в специални картотечни шкафове в заключени помещения. Правата и задълженията на служителите за работа с тях са регламентирани в длъжностните им характеристики. Правата и задълженията на други обработващи лични данни се регламентират в договор. Предоставянето, промяната или прекратяването на оторизиран достъп до регистрите на хартиен носител се контролира от Директора на НМ „Земята и хората“.

(2) Местонахождение на картотечния шкаф - може да бъде поставен в помещение, предназначено за самостоятелна работа на обработващия лични данни или в общо помещение за работа с изпълняващи други дейности, което се заключва.

(3) Достъп до личните данни има само обработващия лични данни.

(4) Обработващият данните се задължава да не предоставя достъп до предоставените му за обработка данни на трети лица, освен в предвидените от закона случаи.

(5) Възможността за предоставяне другому достъп до личните данни при обработката им е ограничена и изрично е регламентирана законово.

**Чл. 10.** (1) Формата на организация и съхраняване на личните данни на технически носител се осъществява чрез тяхното въвеждане на твърд диск на сървъри от компютърната мрежа (в случай, че се обработват от



повече от един служител) или на изолиран компютър (в случай, че се обработват само от един служител или от съответното работно място не може да бъде осигурен достъп до сървър). Компютърът е свързан в локалната мрежа, със защитен достъп до личните данни, с който може да работи само обработващият лични данни и мерки при ниско ниво, съобразно изискванията на Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

(2) При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора на лични данни. Данните се въвеждат в компютъра от хартиен носител.

(3) Достъп до файловете за обработка на лични данни имат само работещите с нея. Носители с лични данни могат да се разпространяват само ако данните са криптирани или ако е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

(4) Защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни електронни носители, както и чрез съхраняване на информацията на хартиен носител. Когато данните се намират на сървър, архивирането им се извършва от служителите по информационно обслужване. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

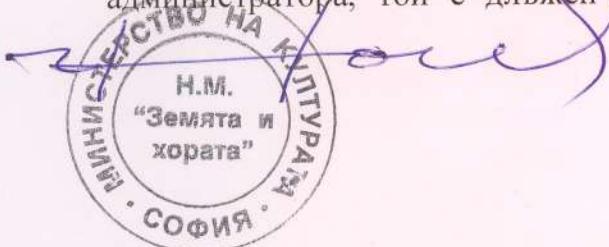
**Чл. 11.** (1) Администраторът на лични данни предприема необходимите технически и организационни мерки, за да защити данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване. Нивото на защита е „ниско“ и „средно“, съобразно изискванията на Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

(2) Администраторът взема специални мерки за защита чрез криптиране, когато обработването включва предаване на данните по електронен път.

(3) Мерките по ал. 1 и 2 са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с обработването, и на естеството на данните, които трябва да бъдат защитени.

(4) Администраторът може да обработва данните сам или чрез възлагане на обработващ данните. Когато е необходимо по организационни причини, обработването може да се възложи на повече от един обработващ данните, включително с цел разграничаване на конкретните им задължения.

(5) В случаите, когато обработването на данните не се извършва от администратора, той е длъжен да определи обработващ данните и да



осигури достатъчни гаранции за тяхната защита.

(7) Отношенията между администратора и обработващия лични данни се уреждат със заповед на администратора или договор, в които се определя обемът на задълженията, възложени от администратора на обработващия данните.

(8) Обработващият лични данни, както и всяко лице, действащо под ръководството на администратора или на обработващия, което има достъп до лични данни, може да ги обработва само по указание на администратора, освен ако в закон е предвидено друго.

(9) След постигане целта на обработване на личните данни администраторът е длъжен да ги:

1. унищожи, или

2. прехвърли на друг администратор, като предварително уведоми за това Комисията за защита на личните данни, ако законът предвижда уведомяване и прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването, или

3. съхранява само в предвидените в закон случаи.

#### **Чл. 12. Мерките за гарантиране нивото на сигурност:**

1. компютърните сървъри за база данни да са на съвременно техническо ниво;

2. компютърните работни конфигурации да използват Desktop операционни системи съобразно изискванията на приложния софтуер за работа с лични данни, да са компетентно балансираны и функционално оптимизирани;

3. за всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите с лични данни, следва да бъдат осигурени непрекъсваеми токозахрънващи устройства (UPS);

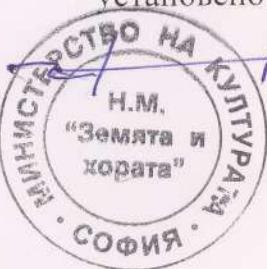
4. минималния набор от системни програмни средства на всяка работна компютърна конфигурация включва:

- Операционна система съобразно изискванията на ползвання приложен софтуер с инсталирани последни пакети за сигурност;
- Антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;
- Активирана защитна стена и deinсталирани комуникатори, осигуряващи достъп извън рамките на компютърната мрежа на НФК и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите;

#### **Чл. 13. Физически мерки за гарантиране нивото на сигурност:**

1. в помещанията, в които са разположени компютърни и комуникационни средства, е осигурена система за ограничаване на достъпа;

2. всички работни помещения се заключват извън рамките на установеното работно време и достъпът до тях е регламентиран. Всички



магнито-оптични носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в шкаф, който се заключва.

**Чл. 14. Организационни мерки за гарантиране нивото на сигурност:**

1. със Заповед Директорът на НМ „Земята и хората“ се определят обработващите лични данни за различните видове регистри, които се водят в НМ „Земята и хората“;

2. организира се охрана на работните помещения в рамките на охраната на цялата сграда (оперативни дежурни).

3. работните компютърни конфигурации, както и цялата ИТ инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;

4. проверка на всички работни компютърни конфигурации по чл. 8 от Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни;

5. пренасянето на лични данни през (чрез) интернет се осъществява чрез електронна поща, като задължително се осигурява криптиране на данните;

6. при ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

**Чл. 15. НМ „Земята и хората“ създава и публикува на електронната си страница Политика за защита на данните, която съдържа:**

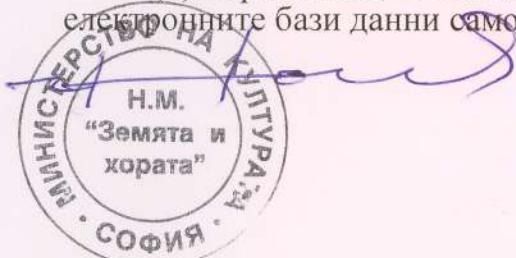
- данни за администратора на лични данни - имена и контакти;
- длъжностно лице по защита на данните - имена и контакти;
- какви категории лични данни се обработват;
- в кои случаи и от кого се получават личните данни;
- за какви цели се обработват личните данни;
- категории получатели, пред които ще се разкриват;
- какви технически и организационни мерки са предприети за защита на данните;
- за какъв период се съхраняват;
- как се архивират и какви са процедурите за унижаване на личните данни;
- правила за действие в случай на нарушение на сигурността на личните данни.

#### **РАЗДЕЛ IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ.**

**Чл. 16. (1)** Обработващите са длъжни да спазват и изпълняват тези правила в съответствие с длъжностните им характеристики.

(2) Обработващият лични данни се задължава да осигури ограничаване на достъпа до помещенията, в които се съхраняват данните само за оторизираните служители чрез заключване на помещенията.

(3) Обработващият лични данни се задължава да осигури достъп до електронните бази данни ~~само~~ по отношение на оторизираните служители .



(4) Обработващият лични данни се задължава да осигури подходяща защита на електронните данни чрез: поддържане на резервно копие, активиране на антивирусна защита.

**Чл. 17.** (1) За обработване на регистри, съдържащи лични данни обработващият подписва декларация, че е запознат със Закона за защита на личните данни, с настоящите правила за защитата на личните данни, които се обработват от него и политиката на НМ „Земята и хората“ за защита на личните данни.

(2) За неизпълнение на задълженията, вменени на съответните длъжностни лица по тези правила и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда или чрез търсене на договорна отговорност, а когато неизпълнението на съответното задължение е констатирано и установено от компетентен орган, предвиденото в Закона за защита на личните данни административно наказание. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

**Чл. 18.** (1) Администраторът предоставя лични данни на друг орган или лице в изпълнение на нормативно установени задължения.

(2) Лични данни се предоставят служебно между служителите в НМ „Земята и хората“ след обосновано искане.

**Чл. 19.** (1) Субектът на данни има право да получава информация от администратора относно обработването на личните му данни:

- в кратка, разбираема и лесно достъпна форма;
- на ясен и прост език;
- писмено или по друг начин, включително с електронни средства, когато е целесъобразно. Устно се получава информацията ако субектът е поискал и самоличноността му е доказана с други средства;
- бесплатно при непрекомерни и основателни искания ;
- без ненужно забавяне, но не по-късно от 1 месец (при необходимост - удължаване на срока с още 2 месеца);
- при ненужно забавяне субектът има право на жалба;
- идентификационни данни за администратора/негов представител и координати за връзка;
- координати на длъжностното лице по защита на лични данни;
- цели на обработване и правно основание;
- законни интереси на администратора, ако поради тази причина се обработват данните;
- получатели или категории получатели на лични данни, ако има;
- намерение да се предават данните на трета държава или на международна организация, ако има;
- срока на съхраняване или критерии за определянето му;
- правото на субекта на: достъп, коригиране или изтриване на личните данни; ограничаване на обработването; да оттегли съгласието си; информация относно правото на жалба;
- доброволен или задължителен характер на предоставянето;



- автоматизирани решения, включително профилиране;
  - цел на по-нататъшното обработване;
  - когато личните му данни са получени при администратора не от самия него, да получи информация за източника на данните.
- (2) Срокове на предоставяне на информацията по ал. 1:
- в разумен срок, но не по-късно от 1 месец (при необходимост - удължаване на срока с още 2 месеца);
  - най-късно при осъществяване на първия контакт, ако данните се ползват за връзка;
  - най-късно при разкриването на друг получател за първи път, ако е предвидено такова.
- (3) Информацията по ал. 1 не се предоставя, ако:
- субектът вече разполага с информацията;
  - предоставянето е невъзможно или изиска несъразмерно големи усилия;
  - получаването или разкриването е изрично разрешено от правото на ЕС или приложимото национално право;
  - личните данни трябва да останат поверителни поради задължение за опазване на професионална тайна съгласно правото на ЕС или приложимото национално право.

**Чл. 20.** Субектът на данните има право на копие на личните данни, които се обработват.

**Чл. 21.** Субектът на данните има право „да бъде забравен“ - право личните данни да бъдат изтрити, когато:

- личните данни не са необходими за целите, за които са събрани или обработвани;
- съгласието е оттеглено и няма друго правно основание;
- субектът на данни възразява срещу обработването;
- обработването е незаконосъобразно;
- с цел изпълнение на нормативно установлено задължение.

**Чл. 22.** Субектът на данните има право на ограничаване на обработването - маркиране на съхранявани лични данни с цел ограничаване на обработването, при определени условия и право на възражение срещу обработването за обществен интерес, официални правомощия, легитимни цели на администратора, включително профилиране, и директен маркетинг.

**Чл. 23.** При установяване на нарушение на сигурността на личните данни, което може да породи висок риск за правата и свободите, НМ „Земята и хората“ уведомява субекта на лични данни без ненужно забавяне за нарушенietо, както и за мерките, които са предприети или предстои да бъдат предприети.

(2) НМ „Земята и хората“ не е длъжен да уведомява субекта на лични данни, ако:

- е предприел подходящи технически и организационни мерки за защита по отношение на данните, засегнати от нарушенietо на сигурността;



- е взел впоследствие мерки, които гарантират, че нарушението няма да доведе до висок риск за правата на субекта на лични данни;
- уведомяването би изисквало непропорционални усилия.

**Чл. 24.** Субектът упражнява правата си по този раздел без това да влияе отрицателно върху правата и свободите на други лица.

**Чл. 25.** При възникване и установяване на инцидент веднага се докладва на Директора на НМ „Земята и хората“.

## **РАЗДЕЛ V ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ**

**Чл.26 .** НМ „Земята и хората“ предприема превантивни действия при защита на личните данни, а именно:

1. защита при аварии – предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или се загребва със собствени подръчни средства.

## **ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

**§ 1.** Настоящите правила се издават на основание Закона за защита на личните данни и Регламент /EC/ 2016/ 679 (General Data Protection Regulation) на Европейския съюз.

**§ 2.** За допуснати нарушения по настоящите правила виновните длъжностни лица носят дисциплинарна и административна отговорност, освен ако деянието не представлява престъпление.

**§ 3.** За неуредените в тези правила въпроси се прилагат разпоредбите на действащата нормативна уредба.

**§ 4.** Контролът по прилагането и спазването на тези правила се осъществява от Директора на НМ „Земята и хората“.

**§ 5.** Настоящите правила влизат в сила от деня на нейното утвърждаване.

Приложение  
Н.М.  
„Земята и  
хората“



## **ДЕКЛАРАЦИЯ**