

УТВЪРДИЛ,
ДИРЕКТОР:

Заличено по ЗЗЛД

(Светлана Еичева)

Заповед № 208-рд-98 от 08.08.2022г.

**ВЪТРЕШНИ ПРАВИЛА
НА НАЦИОНАЛЕН МУЗЕЙ „ЗЕМЯТА И ХОРАТА“
ЗА НАБИРАНЕТО, СЪХРАНЕНИЕТО И ИЗПОЛЗВАНЕТО НА ЛИЧНИ
ДАННИ**

ИСТОРИЯ НА ДОКУМЕНТА

о ед	Наименование на документа нов (Н)/актуализиран (А)	Дата на утвърждаване от директора на МУЗЕЯ	Свързани документи
	Вътрешни правила на Национален музей „Земята и хората“ за набирането, съхранението и използването на лични данни (А)	08.08.2022	Правила относно механизма на обработване и защита на личните данни в НМ „Земята и хората“ - Заповед №136-1-РД-19/28.05.2018

Глава първа ОБЩИ ПОЛОЖЕНИЯ, ПРЕДМЕТ, ЦЕЛ И ПРИНЦИПИ

Чл. 1. Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни, съгласно Общия регламент за защита на данните (Регламент 2016/679) (ОРЗД) и Закона за защита на личните данни (ЗЗЛД), както и организацията, и реда за упражняване на контрол при обработването на лични данни от служителите на Национален музей „Земята и хората“ (за краткост Музея).

Чл. 2. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Общия регламент за защита на данните (Регламент 2016/679) (ОРЗД) и Закона за защита на личните данни и се издават на основание чл.13, ал.1 от Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на лични данни на Комисията за защита на личните данни.

Чл. 3. Вътрешните правила се приемат с цел да регламентират:

1. Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;

2. Видовете регистри, които се водят в Музея и тяхното описание.

3. Необходимите технически и организационни мерки за защита на личните данни на посочените физическите лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).

4. Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

5. Процедури за докладване, управляване и реагиране при инциденти

Чл. 4.(1) Национален музей „Земята и хората“ 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 музеят 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 указаны 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 Музея, не изискват или вече не изискват идентифициране на субекта на данните, Музеят не е задължен 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. Музеят 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 постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. Музеят 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. 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 Музея и/или нормалното му функциониране.

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

Чл. 9. Законосъобразност на обработването:

Съгласие

а) Изпълнение на договор

Когато събранието и обработвани данни са необходими за изпълнението на договор със субекта на данни, *изрично съгласие не е нужно*. Това основание е приложимо в случаите, когато предоставените данни са жизнено важни за изпълнението на договора (напр. сключване на договор за доставка на медикаменти не може да бъде направено без адрес на доставчика).

б) Законово задължение

Когато личните данни са събиращи и обработвани, за да бъде изпълнено законово задължение, *изрично съгласие не е необходимо*. Това основание е приложимо в областта на трудовото, данъчното право и др. нормативни актове.

в) Жизненоважни интереси на субекта на данни

Законосъобразно е да получим и обработим лични данни, ако те са необходими за защита на жизненоважни интереси на субекта на данни или на друго физическо лице, т.е. ще се обработват лични данни на това основание само в случай, че наистина са засегнати жизненоважни интереси, като обстоятелствата ще бъдат детайлно документирани, така че да бъде доказано при необходимост.

г) Изпълнение на задача от обществен интерес

Когато е част от служебно задължение на музея и/или в обществен интерес, съгласие от субекта на данни *няма да бъде поискано*. Преценката дали се касае за обществен интерес и/или служебно задължение, се документира и може да служи като доказателство при необходимост.

д) Легитимен интерес

И в този случай преценката дали един интерес е легитимен и относно степента на засягане на правата и свободите на субектите на данни следва да бъде документирана.

Чл. 10. Когато не са налице хипотезите, посочени в чл. 9, физическите лица, чиито лични данни се обработват от музея, подписват декларация за съгласие по образец.

Чл. 11. (1) Право на достъп до регистрите с лични данни имат само служителите на Музея, съобразно възложените им от закона правомощия, 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 служителите се извършва на база длъжностна характеристика или чрез изричен акт на директора на Музея.

(3) Служителите 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 служители.

Чл. 12. (1) Документите и досиетата, по които работата е приключила, се архивират.

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

(3) Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд.

(4) Документите на електронен носител се съхраняват на специализирани 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 възможността й 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 обработващия/операторът/ на лични данни и оторизираните длъжностни лица.

Чл. 13. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл. 14. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, служителят, констатирал това нарушение, докладва писмено за този инцидент на прекия си ръководител, който от своя страна е длъжен, своевременно да информира ръководството на Музея.

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

Чл. 15. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, Музеят може да определи друго ниво на защита за регистъра и/или допълнителни мерки за защита на информацията от съответния регистър на лични данни.

Чл. 16. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от Музея 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, Музеят 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 директора на Музея и след уведомяване на длъжностното лице по защита на данните.

Чл. 17. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, resp. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, Музеят съобщава в 30-дневен срок от подаване на заявлението, resp. искането.

(3) Срокът по ал. 2 може да бъде удължен от администратора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(4) 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.

(5) Изключение се допуска единствено за тези органи и/или институции, които извършват това въз основа на изискване на закона (напр. МК, МВР, съд, прокуратура, НАП, НОИ и др.).

Глава втора

МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 18. (1) *Физическа защита* в Музея се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни.

(2) Основните приложими организационни мерки за физическа защита в Музея включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на специализирания и административен процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения.

Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, 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. Последните нямат достъп до съхраняваните в електронен вид данни.

Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

Като зони с контролиран достъп се определят всички помещения на територията на музея, в които се събират, обработват и съхраняват лични данни.

Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(3) Основните приложими технически мерки за физическа защита в Музея включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Чл. 19. **(1)** Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на политиката на ръководството на Музея за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
5. съгласие за поемане на задължение за неразпространение на личните данни;

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае“.

(4) Лицата могат да започнат да обработват лични данни след запознаване със:

1. нормативната уредба в областта на защитата на личните данни;
2. политиката и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора.

Чл. 20. **(1)** Основните приложими 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 музея;

2. *Определяне на условията за обработване на лични данни:* личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или

нормалната дейност на Музея, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;

3. *Регламентиране на достъпа до регистрите*: достъпът до регистрите 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 толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.

5. Процедури за унищожаване: Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на Музея, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 21. (1) Защитата на автоматизираните информационни системи и/или мрежи в музея, 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, оценени с ниско ниво на въздействие, включват:

1. *Идентификация* чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на музея. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа „Необходимост да знае“;

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 въвеждане, поддръжка и обработка;

3. *Защитата от вируси*, 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 ИТ специалист.

4. Политиката по *създаване и поддържане на резервни копия за възстановяване* регламентира, предотвратяването на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на Музея.

5. Основни електронни *носители на информация* са: вътрешни твърди дискове, еднократно и/или многократно презписвани външни носители (външни твърди дискове, многократно презписвани карти, памети ленти и други носители на информация, еднократно записвани носители и др.)

6. *Персоналната защита на данните* е част от цялостната охрана на Музея.

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

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

Глава трета

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

Чл. 22. (1) Компютърен достъп 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 парола.

(2) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период. В случай на

отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

Чл. 23. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

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

Чл. 24. (1) В Музея се използва единствено софтуер с уредени авторски права.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.

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

Чл. 25. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпись (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

Глава четвърта

ПОДДЪРЖАНИ РЕГИСТРИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 26. Поддържаните от Национален музей „Земята и хората“ регистри с лични данни са:

1. Регистър „Персонални кадрови данни на служителите в Национален музей „Земята и хората“.
2. Регистър „Дневник за издадените нови трудови книжки.“.
3. Регистър „Регистър на предоставените документи при осигурителя за изчисляване и изплащане на парични обезщетения от ДОО“
4. Регистър „Входящ регистър на обществените поръчки“
5. Регистър „Регистър на договорите склучени в НМЗХ“
6. Регистър „Регистър на оферти по ЗДС и ППЗДС“
7. Регистър „Регистър на даренията и дарителите“

Чл. 27. (1) В регистър „Персонални кадрови данни на служителите в Национален музей „Земята и хората““ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово/служебно правоотношение.

(2) Общо описание на регистър „Персонални кадрови данни на служителите в Национален музей „Земята и хората““

1. Регистърът съдържа следните групи данни:
 - а) социална идентичност - образование и трудова дейност;
 - б) лични данни, които се отнасят до здравето;
 - в) други - лични данни относно гражданско-правния статус на лицата.
2. Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.
3. Предназначенето на събираните данни в регистъра е свързано с :
 - а) Индивидуализиране на трудовите правоотношения;
 - б) Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

в) Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.

г) Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждansки договори.

(3) Технологично описание на регистър „Персонални кадрови данни на служителите в Национален музей „Земята и хората“, като носител на данни:

а) На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудови досиета).

б) На технически носител: Личните данни се въвеждат във файлове тип електронна таблица на компютър.

(4) Определяне на длъжностите: Операторите, обработващи данните в съответните регистри, се определят с писмена заповед на директора на музея.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- а) поверителност - ниско ниво;
- б) цялостност - ниско ниво;
- в) наличност - ниско ниво;
- г) общо за регистъра - ниско ниво.

(6) Срокове на съхранение: Персоналните кадрови данни със срок за дългосрочно запазване се съхраняват в продължение на 50 години, а тези с временни срокове за запазване – 5 години след прекратяване на трудовото правоотношение.

(7) *Организационни мерки за физическа защита* - определено е помещението, в което ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители, с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(8) *Техническите мерки за физическа защита* включват използване на ключалка, шкафове, метални каси, както и оборудване на помещението с пожарогасителни средства.

Трудовите досиета на персонала не се изнасят извън сградата на музея.

Зашитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на музея.

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(9) Предприемане на превантивни действия при защита на личните данни – съставя се план за действие при различните случаи на настъпили форсажорни събития, а именно:

1. Защита при аварии, независещи от музея - 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 загребва със собствени подръчни средства.

(10) Достъп до регистър „Персонални кадрови данни на служителите в Национален музей „Земята и хората““ имат и държавните органи - НАП, НОИ, МЗ, РЗИ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(11) Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изисквали данните по надлежен ред във връзка с изпълнението на техните правомощия.

Чл. 28. (1) В регистър „**Дневник за издадените нови трудови книжки**“ в **Национален музей „Земята и хората“** се набират и съхраняват лични данни на лицата, които работят в Национален музей „Земята и хората“.

(2) Общо описание на регистър „**Дневник за издадените нови трудови книжки**“ в **Национален музей „Земята и хората“**

1. Регистърът съдържа следните групи данни:

- а) социална идентичност - образование и трудова дейност;
- б) лични данни - ЕГН;
- в) други - лични данни относно гражданско-правния статус на лицата.

2. Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството и приложимото законодателство в областта на трудовото право.

3. Предназначенето на събираните данни в регистъра е свързано с :

а) Индивидуализиране на трудовите правоотношения;

б) Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

в) Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.

(3) Технологично описание на регистър „**Дневник за издадените нови трудови книжки**“ в **Национален музей „Земята и хората“**, като носител на данни - на хартиен носител. Данните се набират в писмена (документална) форма и някои се съхраняват в папки (трудови досиета) със съгласието на лицето по трудови правоотношения.

(4) Определяне на длъжностите: Операторите, обработващи данните в съответните регистри, се определят с писмена заповед на директора на музея.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- а) поверителност - ниско ниво;
- б) цялостност - ниско ниво;
- в) наличност - ниско ниво;
- г) общо за регистъра - ниско ниво.

(6) Срокове на съхранение: трудовите книжки се съхраняват до прекратяване на трудовите правоотношения с работещия в НМЗХ, а дневника с издадените трудови книжки е със срок за дългосрочно запазване се съхраняват в продължение на 50 години.

(7) *Организационни мерки за физическа защита* - определено е помещението, в което ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители, с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори

и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(8) Техническите мерки за физическа защита включват използване на ключалка, шкафове, метални каси, както и оборудване на помещението с пожарогасителни средства.

Трудовите досиета на персонала не се изнасят извън сградата на музея.

Заштитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

9) Предприемане на превантивни действия при защита на личните данни – съставя се план за действие при различните случаи на настъпили форсажорни събития, а именно:

1. Защита при аварии, независещи от музея - 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 загребва със собствени подръчни средства.

(10) Достъп до регистър „Дневник за издадените нови трудови книжки в Национален музей „Земята и хората““ имат и държавните органи - НАП, НОИ, МЗ, РЗИ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(11) Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

Чл. 29. (1) В регистър „Регистър на предоставените документи при осигурителя за изчисляване и изплащане на парични обезщетения от ДОО“ се набират и съхраняват лични данни с цел предоставяне на информация пред НОИ за изплащане на паричен обезщетение на леца назначени по трудово правоотношение.

(2) Общо описание на регистър „Регистър на предоставените документи при осигурителя за изчисляване и изплащане на парични обезщетения от ДОО“ в Национален музей „Земята и хората““

1. Регистърът съдържа следните групи данни:

- a) социална идентичност - трудова дейност;

- b) лични данни, които се отнасят до здравето;

2. Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

3. Предназначенето на събираните данни в регистъра е свързано с правилното изчисление на месечното възнаграждение и предосътвяне на данни в НОИ. Съгласно изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

(3) Технологично описание на регистър „Регистър на предоставените документи при осигурителя за изчисляване и изплащане на парични обезщетения от ДОО Национален музей „Земята и хората“, като носител на данни:

- a) На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (болнични листове).

- б) На технически носител: Личните данни се въвеждат във файлове тип и се изпращат в НОИ.

(4) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- a) поверителност - ниско ниво;

- б) цялостност - ниско ниво;

- в) наличност - ниско ниво;

г) общо за регистъра - ниско ниво.

(5) Срокове на съхранение: Персоналните кадрови данни с временни срокове за запазване – 5 години след издаване на болничния лист.

(6) *Организационни мерки за физическа защита* - определено е помещението, в което ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители, с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(7) *Техническите мерки за физическа защита* включват използване на ключалка, шкафове, метални каси.

Болничните листове на персонала не се изнасят извън сградата на музея.

Заштитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При изготвяне на файла за НОИ личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, и след това се предоставят чрез системата на НОИ с електронен подпис.

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(8) Предприемане на превантивни действия при защита на личните данни – съставя се план за действие при различните случаи на настъпили форсажорни събития, а именно:

1. Защита при аварии, независещи от музея - 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 загребва със собствени поддръжни средства.

(9) Достъп до регистър „Регистър на предоставените документи при осигурителя за изчисляване и изплащане на парични обезщетения от ДОО Национален музей „Земята и хората““, имат и държавните органи - НАП, НОИ, МЗ, РЗИ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(10) Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

Чл.30 (1) В регистър „Входящ регистър на обществените поръчки“ се набират и съхраняват данни за проведените обществени пръчи в НМЗХ

(2) Общо описание на регистър „Входящ регистър на обществените поръчки“ в Национален музей „Земята и хората“

1. Регистърът съдържа следните група други - лични данни относно гражданско-правния статус на лицата.
2. Нормативното основание е Закона за обществените поръчки, Законът за счетоводството
3. Предназначението на събираните данни в регистъра е свързано с :

- а) Индивидуализиране на предоставените оферти за всяка едно от процедурите по ЗОП;
- б) Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
- в) Дейностите, свързани със сключване, съществуване, изменение и прекратяване на договорни правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи
- г) Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по договора.

(3) Технологично описание на регистър „Входящ регистър на обществените поръчки“ в Национален музей „Земята и хората“, като носител на данни:

а) На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки .

б) На технически носител: Личните данни се въвеждат и в електроната система за обществени поръчки ЕОП.

(4) Определяне на длъжностите: Операторите, обработващи данните в съответните регистри, се определят с писмена заповед на директора на музея.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- а) поверителност - ниско ниво;
- б) цялостност - ниско ниво;
- в) наличност - ниско ниво;
- г) общо за регистъра - ниско ниво.

(6) Срокове на съхранение: офертите и съществуващите ги документи се пазят със срок за дългосрочно запазване се съхраняват в продължение на 10 години.

(7) Организационни мерки за физическа защита - определено е помещението, в което ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители, с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(8) Техническите мерки за физическа защита включват използване на ключалка, шкафове, метални каси, както и оборудване на помещението с пожарогасителни средства.

Трудовите досиета на персонала не се изнасят извън сградата на музея.

Заштитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(9) Предприемане на превантивни действия при защита на личните данни – съставя се план за действие при различните случаи на настъпили форсажорни събития, а именно:

1. Защита при аварии, независещи от музея - 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 загребва със собствени подръчни средства.

(10) Достъп до регистър „**Входящ регистър на обществените поръчки**“ в Национален музей „Земята и хората“ имат държавните органи - АДФИ, ВЪТРЕШЕН СМЕТНА ПАЛАТА, ОДИТ към МК и др. за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(11) Достъп до обработваните данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

Чл.31 (1) В регистър „Регистър на договорите склучени в НМЗХ“ се набират и съхраняват данни за склучените договори в НМЗХ с юридически и физически лица за стоки или услуги.

(2) Общо описание на регистър „Регистър на договорите склучени в НМЗХ“

1. Регистърът съдържа следните групи други - лични данни относно гражданско-правния статус на лицата.

2. Нормативното основание е, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на гражданско-правното законодателство.

3. Предназначението на събираните данни в регистъра е свързано с :

а) Индивидуализиране на договорите за стоки и услуги;

б) Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

в) Дейностите, свързани със сключване, съществуване, изменение и прекратяване на договорните правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи по граждански договори, служебни бележки, справки, удостоверения и др.

г) Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по договорните правоотношения и по граждански договори.

(3) Технологично описание на регистър „Регистър на договорите склучени в НМЗХ“, като носител на данни:

а) На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папка - договори.

б) На технически носител: Личните данни се въвеждат във файлове тип електронна таблица на компютър.

(4) Определяне на длъжностите: Операторите, обработващи данните в съответните регистри, се определят с писмена заповед на директора на музея.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

а) поверителност - ниско ниво;

б) цялостност - ниско ниво;

в) наличност - ниско ниво;

г) общо за регистъра - ниско ниво.

(6) Срокове на съхранение: данните за склучените договори се съхраняват 10 години след приключване на договорните правоотношения.

(7) Организационни мерки за физическа защита - определено е помещението, в което ще се обработват и съхраняват данните по договорите, като физическия достъп е ограничен само за служители, с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори

и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(8) Техническите мерки за физическа защита включват използване на ключалка, шкафове, метални каси.

Заштитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(9) Предприемане на превентивни действия при защита на личните данни – съставя се план за действие при различните случаи на настъпили форсажорни събития, а именно:

1. Защита при аварии, независещи от музея - 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 загребва със собствени подръчни средства.

(10) Достъп до регистър „Регистър на договорите сключени в НМЗХ“ имат държавните органи – АДФИ, СМЕТНА ПАЛАТА, МК и др. за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(11) Достъп до обработваните данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изисквали данните по надлежен ред във връзка с изпълнението на техните правомощия.

Чл.32 (1) В регистър „Регистър на оферти по Закон за държавната собственост и ППЗДС“ се съхраняват и

(2) Общо описание на регистър „Регистър на оферти по ЗДС и ППЗДС“ в Национален музей „Земята и хората“

1. Регистърът съдържа следните групи други - лични данни относно гражданско-правния статус на лицата.
2. Нормативното основание е ЗДС, Законът за счетоводството и приложимото законодателство.
3. Предназначението на събираните данни в регистъра е свързано с :
 - а) Предоставяне на информация в НАП, МК , НИНКН и други институции;
 - б) Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

(3) Технологично описание на регистър „Регистър на оферти по ЗДС и ППЗДС“ в Национален музей „Земята и хората“, като носител на данни:

- а) На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папка.
- б) На технически носител: данните се въвеждат във файлове тип електронна таблица на компютър.

(4) Определяне на длъжностите: Операторите, обработващи данните в съответните регистри, се определят с писмена заповед на директора на музея.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- а) поверителност - ниско ниво;
- б) цялостност - ниско ниво;
- в) наличност - ниско ниво;

г) общо за регистъра - ниско ниво.

(6) Срокове на съхранение: Данни се съхраняват със срок 10 години.

(7) Техническите мерки за физическа защита включват използване на ключалка, шкафове, метални каси, както и оборудване на помещението с пожарогасителни средства.

Заштитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При внедряване на нов програмен продукт за обработване на данни се проверяват възможностите на продукта с оглед спазване изискванията за осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(8) Предприемане на превантивни действия при защита на данните – съставя се план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. Защита при аварии, независещи от музея - 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 загребва със собствени подръчни средства.

(9) Достъп до регистър „Регистър на оферти по ЗДС и ППЗДС“ в Национален музей „Земята и хората“ имат и държавните органи - НАП, АДФИ, СМЕТНА ПАЛАТА, МК, НИНКН и др. за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(10) Достъп до обработваните данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изисквали данните по надлежен ред във връзка с изпълнението на техните правомощия.

Чл.33 (1) В регистър „Регистър на даренията и дарителите“

(2) Общо описание на регистър „Регистър на даренията и дарителите“ в Национален музей „Земята и хората“

1. Регистърът съдържа следните групи други - лични данни относно гражданско-правния статус на лицата.
2. Нормативното основание е Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство .
3. Предназначенето на събираните данни в регистъра е свързано с :
 - а) Индивидуализиране на даренията;
 - б) Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
 - в) Дейностите, свързани със сключване, съществуване, изменение и прекратяване на дарителските правоотношения, изготвяне на договори, анекси, справки, удостоверения и др.
 - г) Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се.

(3) Технологично описание на регистър „Регистър на даренията и дарителите,, в Национален музей „Земята и хората“, като носител на данни:

а) На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (договори или дарители).

б) На технически носител: Личните данни се въвеждат във файлове тип електронна таблица на компютър.

(4) Определяне на длъжностите: Операторите, обработващи данните в съответните регистри, се определят с писмена заповед на директора на музея.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- а) поверителност - ниско ниво;
- б) цялостност - ниско ниво;
- в) наличност - ниско ниво;
- г) общо за регистъра - ниско ниво.

(6) Срокове на съхранение: запазване и съхраняване в продължение на 10 години,

(7) *Организационни мерки за физическа защита* - определено е помещението, в което ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители, с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(8) *Техническите мерки за физическа защита* включват използване на ключалка, шкафове, метални каси.

Заштитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(9) Предприемане на превантивни действия при защита на личните данни – съставя се план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. Защита при аварии, независещи от музея - 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 загребва със собствени подръчни средства.

(10) Достъп до регистър „Персонални кадрови данни на служителите в Национален музей „Земята и хората“ имат и държавните органи - НАП, СМЕТНА ПАЛАТА, АДФИ и др. за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(11) Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

Глава пета

ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 34. (1) Дължностно лице по защита на данните се определя от директора на музея.

(2) Дължностно 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 регистрация 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 инсталлиран софтуер, на 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. 35. Служителите на музея 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. 36. (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 музея или за трето лице, на този служител може да се потърси отговорност по реда на общото гражданско законодателство.

Глава шеста ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 37. Всички служители на музея 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. 38.(1) За всички неурядени 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:

1. Документ I-04-03-01 - Декларация-съгласие за обработка на лични данни (*която се подписва, когато обработването се извършива на друго основание, непредвидено в чл. 6, б. "б" – б. "е" от Регламент 2016/679*);
2. Документ I-04-03-02 - Декларация за оттегляне на съгласие;

3. Документ I-04-03-03 - Протокол за унищожаване на лични данни и носители на лични данни;
4. Документ I-04-03-04 - Декларация от служителите за опазване на лични данни;
5. Документ I-04-03-05 - Заявление за достъп до лични данни;
- Чл. 39.** Настоящите вътрешни правила са утвърдени със Заповед на директора на Национален музей „Земята и хората“

Глава седма

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. По смисъла на настоящите правила:

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 признания, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

2) „**обработване**“ 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, извлечане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

3) „**ограничаване на обработването**“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

4) „**профилиране**“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочтения, интереси, надеждност, поведение, местоположение или движение;

5) „**псевдонимизация**“ означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани 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;

6) „**регистър с лични данни**“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален принцип;

7) „**администратор**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни;

8) „**обработващ лични данни**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

9) „**получател**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не.

10) „**трета страна**“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия

лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

11) „**съгласие на субекта на данните**“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

12) „**нарушение на сигурността на лични данни**“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

13) „**генетични данни**“ означава лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;

14) „**биометрични данни**“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

15) „**данни за здравословното състояние**“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние.