ВЪТРЕШНИ ПРАВИЛА НА
РЕГИОНАЛЕН ИСТОРИЧЕСКИ МУЗЕЙ
„СТОЮ ШИШКОВ“ – СМОЛЯН
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ПРЕДМЕТ

Чл. 1. (1) Настоящите Вътрешни правила (**Правилата**) определят реда, по който **РИМ „Стою Шишков“ (Музеят),** с адрес на регистрация: Смолян, ул. Дичо Петров“ № 3, с **ЕИК 000608629** събира, записва, организира, структурира, съхранява, адаптира или променя, извлича, консултира, използва, разкрива чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подрежда или комбинира, ограничава, изтрива, унищожава или обработва по друг начин лични данни за целите на своята дейност.
(2) В зависимост от конкретната ситуация **Музеят** може да обработва данни в качеството на администратор или обработващ.
(3) Правилата са изготвени в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

Чл. 2. Настоящите **Правила** уреждат:
(1) Принципите, процедурите и механизмите за обработка на личните данни;
(2) Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;
(3) Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;
(4) Лицата, които обработват лични данни, и техните задължения;
(5) Правилата за предаване на лични данни на трети лица в България и чужбина;
(6) Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;
(7) Техническите ресурси, прилагани при обработката на лични данни.

ДЕФИНИЦИИ

Чл. 3. За целите на настоящите Правила, използваните понятия имат следното значение:
• **ЗЗЛД –** Закон за защита на личните данни.
• **КЗЛД** – Комисия за защита на личните данни.
• **ОРЗД** – Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

• **Длъжностно лице по защита на данните** – физическо лице или организация, определени съгласно изискванията на чл. 37 и сл. от ОРЗД.
[или – ако не е задължително определянето на длъжностно лице по защита на данните – алтернативно може да се включи:
• ***Лице, отговорно за личните данни*** *– лице, което е служител в* **Музея** *изпълнява функции по поръчение, на което са възложени задълженията във връзка със защитата и процесите по обработка на лични данни, уредени в тези Правила. Основните дейности на администратора или обработващия лични данни не се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни или в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения. С оглед това обстоятелство,* **Музеят** *няма задължение да назначи длъжностно лице по защита на данните и не следва да се счита, че е назначил такова лице или че лицето, отговорно за личните данни, има задълженията и следва да отговаря на изискванията на лицето по смисъла на чл. 37 и сл. от ОРЗД.]*
• **Администратор на лични данни** – 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. В настоящите Правила „администратор“ обозначава **Музеят.**
• **Обработващ лични данни** – лице или организация, което въз основа на договор обработва лични данни, предоставени от **Музея** за уговорените цели.
• **Известия по защита на данните** – отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който **Музея** събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на организацията), така и отнасящи се до обработване със специфична цел.
• **Обработване на данни** – всяка дейност, която е свързана с използването на лични данни. Това включва: получаване, записване, съхранение, извършване на операция или серия от операции с данните като напр. организиране, редактиране, възстановяване, използване, предоставяне, изтриване или унищожаване. Обработването също включва и трансфер на лични данни до трети лица.
• **Псевдоминизиране** – заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече идентификатори („псевдоними”), така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.
• **Съгласие** – всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на лични данни, свързани с него.

СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 4. (1) **Музеят** събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, доставчик на услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от **Музея**, са групирани в регистри на дейностите по обработване, съдържащи правила за обработване на лични данни, отнасящи се до:

- работници и служители и изпълнители по граждански договори;

- кандидати за работа;
- потребители на услуги;
- доставчици на услуги;
- посетители на музейната експозиция.

(2) Относно **лицата, заети по трудови или граждански правоотношения в Музея и на кандидатите за работа**, се събират следните лични данни:
а) Идентификация: име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни;
б) Образование и професионална квалификация; данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;
в) Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;
г) Други данни: свидетелство за съдимост, когато се изисква представянето му съгласно нормативен акт, както и други данни, чието обработване е необходимо за изпълнение на правата и задълженията на **Музея** като работодател.
(3) Относно физически лица, **потребители на услуги на Музея,** се събират лични данни, които са необходими за изпълнението на законовите задължения на **Музея** като доставчик на услуги, както следва:
• име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни.
(4) Относно физически лица, **доставчици на услуги на Музея,** се съхраняват лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на дружеството от външни доставчици, както следва:
• име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни; електронна поща.
(5) Относно физически лица, **посетителите на музейната експозиция** се съхраняват лицата им, които се заснемат от видео наблюдение в залите, необходимо за изпълнението на законовите задължения на **Музея** и с оглед опазване сигурността на експонатите.
(6) **Музеят** обработва чувствителни данни, само доколкото това е необходимо за изпълнение на специфичните му права и задължения в областта на трудовото и осигурително законодателство.

ЦЕЛИ И ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 5. Целите на обработването на лични данни са:
(1) управление на човешките ресурси, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на **Музея** в качеството му на работодател;
(2) администриране на отношенията с потребители на услуги на **Музея** и предоставяне на услуги;
(3) сключване и изпълнение на договори с доставчици за предоставяне на услуги на **Музея;**
(4) охрана на движими културни ценности, показани в експозицията на **Музея.**
Чл. 6. Личните данни се обработват законосъобразно, добросъвестно и прозрачно при спазване на следните принципи:

(1) Субектът на данните се информира предварително за обработването на неговите лични данни;
(2) Личните данни се събират за конкретни, точно определени и законни цели и не се обработват допълнително по начин, несъвместим с тези цели;
(3) Личните данни съответстват на целите, за които се събират;
(4) Личните данни трябва да са точни и при необходимост да се актуализират;
(5) Личните данни се заличават или коригират, когато се установи, че са неточни или не съответстват на целите, за които се обработват;
(6) Личните данни се поддържат 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. 7. За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:
(1) Субектът на данните е информиран и е дал своето съгласие;
(2) Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
(3) Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
(4) Обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;
(5) Обработването е необходимо за изпълнение на задача от обществен интерес;
(6) Обработването е необходимо за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. Целите, за които се обработват лични данни на това основание, трябва да са описани в приложимите известия по защита на данните.

СЪГЛАСИЕ

Чл. 8. (1) Субектът на данни е съгласен с обработването, ако изрази това ясно и недвусмислено – чрез изявление или друг потвърждаващ акт. Ако съгласието за обработка на лични данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси.
(2) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време, и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.
(3) Декларациите за съгласие се съхраняват от дружеството, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност.

ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Процедура за обработване на личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в* Музея, *както и на кандидатите за работа
Чл. 9. (1) Личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в **Музея,** както и на кандидатите за работа, се събират при и по повод

набирането на персонал. Данните на всеки работник и служител на Дружеството се съхраняват в лични досиета, като някои данни могат да се съхраняват или обработват и на технически носител. Данните от проведени конкурси и интервюта се съхраняват на технически и/или хартиен носител, в зависимост от нуждата.
(2) Личните досиета се подреждат в специални картотечни шкафове със заключване, находящи се в кабинета на Лицето, отговорно за личните данни. Данните на кандидатите за работа, които се съхраняват на хартиен носител, се съхраняват в нарочни шкафове в кабинета на Лицето, отговорно за личните данни. Достъпът до кабинета се предоставя само на лицата, оправомощени да обработват личните данни, като за целта се създава специален ред за влизане в помещението чрез ключ, магнитна карта или друго подходящо средство и/или устройство.
(3) Лицата, оправомощени да обработват лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните досиета и класьорите с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.
(4) Досиета на работниците и служителите, както и данните на кандидатите за работа, не се изнасят извън сградата на дружеството.

Процедура за обработване на лични данни, отнасящи се до клиенти и доставчици на услуги

Чл. 10. (1) Личните данни, отнасящи се до клиенти, се събират при подаване на заявка за предоставяне на услуга или сключване на договор с потребител на услуги на **Музея.**
(2) Личните данни, отнасящи се до доставчици на услуги, се събират при сключване на договор с доставчик на услуги, като обичайно личните данни се съдържат в текста на самите договори.
(3) Личните данни се съхраняват на електронен и хартиен носител (подписани копия на сключените договори), които се класират в отделни досиета. Досиетата се съхраняват в каси, които се заключват от Лицето, отговорно за личните данни. Електронните данни се съхраняват в бази данни на компютър, до който има достъп само Лицето, отговорно за личните данни.

Процедура за обработване на лични данни, отнасящи се до посетители на музейната експозиция

Чл. 11. (1) Видеозаснемане на лицата, посетили експозицията на **Музея,** се съхраняват в сървъра на системата за видеонаблюдение в срок от една година.

ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл. 12. (1) **Музеят** документира дейностите по обработване на лични данни при спазване на принципа на отчетност.
(2) Документацията трябва да е достатъчна, за да докаже спазването на принципите за законосъобразно обработване на личните данни.
(3) Обработването на данни, свързано с предаване на данни на обработващи, установени в страната или чужбина; съхранение на данни на сървъри, собственост на трети лица; архивиране или изтриване на данни; въвеждане на псевдонимизация, както и всяка друга

обработка, чиито параметри са различни от описаните в тези правила, се документира чрез създаване на протоколи, които съдържат следната информация:
(а) целите на обработването;
(б) категориите лични данни и категориите субекти на данни;
(в) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави;
(г) предаването на лични данни на трета държава;
(д) когато е възможно, предвидените срокове за изтриване на различните категории данни;
(е) общо описание на техническите и организационни мерки за сигурност.
(4) Протоколите се изготвят от лицата, които извършват съответната обработка на данни по указания от Лицето, отговорно за личните данни.
(5) Съвкупността от всички протоколи, съдържащи гореописаната информация, съставлява регистъра на дейностите по обработването, съгласно чл. 30 от ОРЗД.

МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Технически мерки
Чл. 13. (1) Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа. Възможните технически средства за контрол на достъпа са:
- охрана на помещенията;
- устройства за разпознаване чрез магнитна карта и/или ключ;
- наблюдение с видеокамери в коридорите;
- политика на допускане на външни лица до административните помещения на **Музея е** само с придружител от персонала на **Музея.**
(2) Помещенията на **Музея** са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.

Мерки за документална защита
Чл. 14. (1) **Музеят** установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани в тези Правила. За отделни категории данни може да се предвиди псевдонимизиране по предложение на Лицето, отговорно за личните данни.
(2) Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители при възникнала необходимост.

Персонални мерки на защита
Чл. 15. (1) Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни в **Музея**:
- поемат задължение за неразпространение на личните данни, до които имат достъп;
- се запознават с нормативната база, вътрешните правила и политики на **Музея** относно защитата на личните данни;
- преминават обучение за реакция при събития, застрашаващи сигурността на данните;
- са инструктирани за опасностите за личните данни, които се обработват от **Музея;**
- се задължават да не споделят критична информация помежду си и с външни лица, освен по установения с тези Правила ред.

(2) При постъпване на работа всички служители преминават обучение за реакция при събития, застрашаващи сигурността на данните, и обучение относно задълженията на **Музея,** свързани с обработката на лични данни, и мерките за защита на данните, които следва да предприемат в процеса на работа. Последващи обучения и тренировки на персонала се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.

Мерки за защита на автоматизирани информационни системи и криптографска защита

Чл. 16. (1) Достъп до операционната система, съдържаща файлове с лични данни, имат само лица от **Музея**, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.
(2) Електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично и др.
(3) Архивиране на личните данни на технически носител се извършва периодично с оглед съхранение на информацията.

Чл. 17. (1) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия, др., се осигурява посредством:
- въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни, и файловете, които съдържат лични данни;
- антивирусни програми, проверки за нелегално инсталиран софтуер;
- периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;
- периодично архивиране на данните на технически носители, поддържане на информацията на хартиен носител (архивни копия).
(2) Лицето, отговорно за личните данни, докладва периодично на ръководството на **Музея** предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 18. (1) Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на Лицето, отговорно за личните данни, като му предоставят цялата налична информация.
(2) Лицето, отговорно за личните данни, извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.
(3) Лицето, отговорно за личните данни, докладва незабавно на ръководството на **Музея** наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.
(4) След съгласуване с ръководството на **Музея**, Лицето, отговорно за личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, Лицето, отговорно за личните данни, може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай Лицето, отговорно за личните данни, уведомява незабавно ръководството за предприетите мерки и съобразява последващи действия с получените инструкции.

Чл. 19. (1) В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от ръководството на **Музея**, Лицето, отговорно за личните данни, организира уведомяването на КЗЛД.
(2) Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението.
(3) Уведомлението до КЗЛД съдържа следната информация:
(а) описание на нарушението на сигурността; категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
(б) името и координатите за връзка на Лицето, отговорно за личните данни;
(в) описание на евентуалните последици от нарушението на сигурността;
(г) описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.
(4) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Лицето, отговорно за личните данни, без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

Чл. 20. (1) **Музеят** води регистър на нарушенията на сигурността, който съдържа следната информация:
(а) дата на установяване на нарушението;
(б) описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);
(в) описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;
(г) предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за **Музея;**
(д) предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.
(2) Регистърът се води в електронен формат от Лицето, отговорно за личните данни.

ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 21. (1) **Музеят** може при необходимост да предоставя лични данни на трети лица, действащи в качеството на обработващ, въз основа на изричен договор.
(2) В случаите на предоставяне на данните на служители, клиенти или доставчици на услуги на обработващ, **Музеят:**
(а) изисква достатъчно гаранции от обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;

(б) сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламент (ЕС) 2016/679;
(в) информира физическите лица, чиито данни ще бъдат предоставени на обработващ.
(3) Обработване на лични данни от обработващи извън ЕС/ЕИП е допустимо само когато:
(а) Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансферът, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;
(б) Налице са подходящи мерки за защита – като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм;
(в) Субектът на данни е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове, или
(г) Трансферът е необходим за една от целите, изброени в ОРЗД, включително изпълнението на договор със субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие.

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 22. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от **Музея.** Оценка на въздействието се извършва за високорискови дейности по обработване.
(2) Оценка на въздействието е необходимо при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с обработване на лични данни, включително:
- първоначалното въвеждане на нови технологии или прехода към нови технологии;
- автоматизирано обработване, включително профилиране или автоматизиране вземане на решения;
- обработване на чувствителни лични данни в голям мащаб;
- мащабно, систематично наблюдение на публично обществена зона.
(3) За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 23. (1) Унищожаване на личните данни се извършва от **Музея** или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове.
(2) Информацията в регистрите се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.
(3) Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина.
(4) Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

ЛИЦА, ОТГОВАРЯЩИ ЗА СЪБИРАНЕТО, ОБРАБОТКАТА И СЪХРАНЕНИЕТО НА ЛИЧНИТЕ ДАННИ И ДОСТЪП ДО ЛИЧНИ ДАННИ

Чл. 24. Лицето, отговорно за личните данни, и лицата, обработващи личните данни от името на **Музея**, са физически или юридически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт, включително и чрез настоящите Правила.

Чл. 25. Лицето, отговорно за личните данни:
- подпомага **Музея** и лицата, обработващите личните данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на данните;
- осигурява нормалното функциониране на гореспоменатите системи за защита;
- осъществява контрол през целия процес на събиране и обработване на данните;
- изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;
- периодично изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;
- уведомява **Музея** своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;
- унищожава данните от хартиените и техническите носители съгласно закона и сроковете, установени в тези Правила;
- преупълномощава физически или юридически лица с писмен акт, които да осъществяват защитата на личните данни.

Чл. 26. (1) Събирането, обработката, съхранението и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.
(2) При възлагане на дейности, налагащи обработката на лични данни от регистрите на **Музея,** доставчиците на услуги следва да спазват приложимите нормативни изисквания относно обработката на личните данни и процедурите на чл. 19 от тези Правила.
(3) Достъп до личните данни могат да имат и съответните държавни органи – съд, следствие, прокуратура, ревизиращи органи и др. Гореспоменатите могат да изискат данните по надлежен ред във връзка с изпълнението на техните правомощия.

ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 27. (1) Всяко лице има право да иска достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.
(2) Правото на достъп се осъществява чрез искане на засегнатото физическо лице, получено на адреса по седалището на **Музея** или официалната електронна поща.
(3) Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на негови лични данни, обработването на които не отговаря на изискванията на закона.

(4) Всяко лице има право писмено да възрази срещу обработването на и/или предоставянето на трети лица на неговите лични данни без необходимото законово основание.
(5) **Музеят** е длъжен в двуседмичен срок от получаване на искане по предходните алинеи да уведоми заявителя дали са налице законовите основания за уважаване на искането. Ако **Музеят** установи, че са налице законовите основания да уважи искането, уведомява лицето и за реда, по който може да упражни правото си.
(6) Субектите на данни имат също правото да:
- оттеглят съгласието си за обработване по всяко време;
- възразят срещу употреба на личните им данни за целите на директния маркетинг;
- изискат информация за основанието, въз основа на което личните им данни са предоставени за обработване на обработващ извън ЕС/ЕИП;
- възразят срещу решение, взето изцяло на база на автоматизирано обработване, включително профилиране;
- бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;
- подават жалби до регулаторния орган;
- в някои случаи да получат или да поискат техните лични данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене (право на преносимост).

ПРОМЕНИ НА ВЪТРЕШНИТЕ ПРАВИЛА

Чл. 28. **Музеят** може да променя тези Правила по всяко време. Всички промени следва да бъдат незабавно сведени до знанието на лицата, които засягат.

Настоящите Правила са приети и влизат в сила на деня на подписването им.

За и от името на Регионален исторически музей „Стою Шишков“ – Смолян:

_____
[Таня Марева - директор]

18 май 2018 г.
Смолян