РЕПУБЛИКА БЪЛГАРИЯ

МИНИСТЕРСТВО НА ФИНАНСИТЕ

Утвърдена със
Заповед № ЗМФ-817/30.08.2018 г.

П О Л И Т И К А
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
В МИНИСТЕРСТВОТО НА ФИНАНСИТЕ

Администратор	дата	версия	обем
Министерство на финансите *Уебсайт:* *http://www.minfin.bg/*	м. август, 2018 г.	1.0	стр. 17

Контакт с длъжностното лице за защита на личните данни:		
ДЛЗД/Отговорник: Мирослав Коларов	E-mail: m.kolarov@minfin.bg	Телефон: +359 2 9859 2512

История на промените на документа

Версия	Дата	Описание на допълненията и измененията	Наименование, номер и дата на документа, с който версията е одобрена
1.0	**30.08.2018 г.**	Политика за защита на личните данни в Министерството на финансите	Заповед № ЗМФ-817/30.08.2018 г. на министъра на финансите

Обща информация за документа

Контрол	Администратор на лични данни – Министерството на финансите чрез министъра на финансите; Длъжностно лице по защита на данните (ДЛЗД) – определено със заповед на министъра на финансите; Надзорен орган – Комисията за защита на личните данни, независим публичен орган, създаден от държава членка съгласно чл. 51 от ОРЗД.
Цел	Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните - ***ОРЗД***) замества Директивата 95/46 / ЕО за защита на данните, който има пряко действие и предполага изменение в законодателството на страните -членки в областта на защитата на личните данни. Неговата цел е да защитава правата и свободите на физическите лица и да гарантира, че личните данни не се обработват без тяхно знание и когато е възможно, че се обработват с тяхно съгласие.
Обхват	***Материален обхват*** (чл. 2 от ОРЗД) – ОРЗД се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (например ръчно и на хартия), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни. ***Териториален обхват*** (чл. 3 от ОРЗД) – правилата на ОРЗД важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност. Прилага се и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС. *Принципът, е че правилата на ОРЗД „следват“ личните данни на субектите на данни, които се намират в Европейския съюз.*
Разпространение	Всички служители в МФ, които събират, записват, организират, структурират, съхраняват, адаптират или променят, извличат, консултират, разкриват чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждат или комбинират, ограничават, изтриват или унищожават лични данни, във връзка с изпълняваната служебна дейност.
Достъп до актуалната версия	Чрез интранет страницата на МФ, раздел „Защита на личните данни в МФ“; Чрез файловия сървър: *MF (\\mfshare) R:\ОБЩИ ПРОЕКТИ НА МФ\Защита на личните данни*

Понятия

Лични данни	Всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице, както и всяка друга информация, която се определя от приложимото право като лични данни.
Специални категории лични данни (чувствителни данни)	Лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни, отнасящи се до здравето, или данни относно сексуалния живот на физическо лице или сексуална ориентация, както и всички други лични данни, които се определят от приложимото право като специални.
Администратор	Всяко 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; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.
Обработващ лични данни	Означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора (чл. 4, т. 8 от ОРЗД).
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, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.
Субект на данните	Всяко живо физическо лице, което е предмет на личните данни, съхранявани от администратора.
Съгласие на субекта на данните	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.
Дете	Всяко лице на възраст под 16 години, въпреки че възрастта може да бъде друга, съгласно правото на държавата-членка. Обработката на лични данни на едно дете е законна, само ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или е упълномощен да даде съгласието си.

Профилиране	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 предпочитания, интереси, надеждност, поведение, местоположение или движение.
Нарушение на сигурността на лични данни	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.
Основно място на установяване	Седалището на администратора в ЕС е мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващия лични данни в Съюза, където се осъществяват основните дейности по обработването.
Получател	Физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването.
Трета страна	Всяко 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.

С ъ д ъ р ж а н и е

ГЛАВА I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящата политика за защита на личните данни (наричана „Политиката“) има за цел да гарантира, че личните данни се обработват в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Общ регламент относно защитата на данните (ОРЗД), който регулира обработването на лични данни на физически лица в рамките на ЕС от физическо лице, дружество или организация, Закона за защита на личните данни (ЗЗЛД) и приложимите нормативни актове, регламентиращи защита на личните данни.

(2) Политиката се прилага за обработване на лични данни изцяло или частично с автоматизирани средства, както и за обработването с други средства, които са част от Единния регистър на данни в МФ, който включва всички категории дейности по обработване чрез информационни системи или с други средства.

(3) Политиката не се прилага за данни, обработвани от служители на МФ поради причини от чисто личен характер, или за дейности, извършвани у дома при условие, че няма връзка с професионална или служебна дейност.

(4) МФ декларира, че спазва основните права и положения, свързани с процеса по събиране и обработване на лични данни за конкретната цел и във всеки конкретен случай (*Приложение № 1*).

Чл. 2. (1) При обработването на лични данни се спазват следните принципи:

1. законосъобразност – данните се обработват при наличие на някое от следните основания:

а) *правно задължение:* обработването е необходимо, за да може администраторът да изпълни законово задължение (без да се включват договорни задължения);

б) *договор:* обработването е необходимо за изпълнението на договор, по който субектът на лични данни е страна, или за предприемане на конкретни стъпки преди сключването на такъв договор;

в) *съгласие*: лицето следва да е дало ясно съгласие за обработването на личните данни за конкретна цел и операцията за обработване *(Приложение № 2*);

г) *важни интереси:* обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) *обществена задача:* обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора, а задачата или функцията има ясна правна основа;

е) *законни (легитимни) интереси:* обработването е необходимо с цел защита на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни (напр. когато субектът на данни е дете или се касае до специални категории лични данни), или МФ обработва данни в изпълнение на правомощията на министъра;

2. добросъвестност – на субектите на данни следва да се предостави определена информация, необходима във всеки конкретен случай и за всяка конкретна цел, по разбираем, кратък и достъпен начин;

3. прозрачност – всяка информация във връзка с обработването да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки. Този принцип се отнася в особена степен за информацията, която получават субектите на данни за администратора, целите на обработването и за допълнителната информация, гарантираща добросъвестно и прозрачно обработване на данните по отношение на засегнатите физически лица и тяхното право да получат потвърждение и уведомление за съдържанието на свързани с тях лични данни, които се обработват;

4. ограничение на целите – данните са събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или

исторически изследвания или за статистически цели не се счита, съгласно чл. 89, § 1 от ОРЗД, за несъвместимо с първоначалните цели;

5. свеждане на данните до минимум – обработването да е адекватно (подходящо) на конкретната цел, за която се обработват данните;

6. точност – гарантира, че данните са точни и са поддържани в актуален вид, както и своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;

7. ограничение на съхранението – да се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно чл. 89, § 1 от ОРЗД при условие, че бъдат приложени подходящите технически и организационни мерки с цел да бъдат гарантирани правата и свободите на субекта на данните;

8. цялостност и поверителност – да са обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки;

9. отчетност – гарантира спазването на задълженията, произтичащи от извършването на оценки на въздействието върху защитата на личните данни и от предварителната консултация с надзорния орган. Води се Регистър на дейностите по обработване на лични данни и се попълват съответните уведомления от администратора до надзорния орган.

(2) При всички положения администраторът трябва да докаже, че има правно основание, за да обработва личните данни на субектите.

ГЛАВА II
ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ
Раздел I
Оценка на въздействието

Чл. 3. (1) Оценката на въздействието върху защитата на данните (ОВЗД) е процес, при който администраторът преценява нивата на рисковете за правата и свободите на субектите на данни, а именно степента (нивото) на въздействие, което нарушаването на поверителността, цялостността или наличността на личните данни би оказало върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица.

(2) Администраторът извършва ОВЗД с цел определяне на:

1. адекватно ниво на технически и организационни мерки за защита на личните данни, което отговаря на обработваните лични данни и въздействието при нарушаване на защитата им;

2. най-ефективния начин за спазване на задълженията на служителите в МФ за защита на данните.

Чл. 4. (1) ОВЗД трябва да съдържа най-малко следната информация:

1. описание на операциите по обработване и целите, включително, когато е приложимо, законните интереси, преследвани от администратора;

2. оценка на необходимостта и пропорционалността на операциите по обработване във връзка с целта;

3. оценка на рисковете за правата и свободите на субектите на данни, които е вероятно да възникнат от обработването (и по-специално произхода, естеството, особеностите и тежестта на тези рискове);

4. мерките, предвидени за справяне с рисковете, включително предпазни мерки за сигурност и механизми за гарантиране на защитата на личните данни и доказване на спазването на разпоредбите на ОРЗД;

5. оценката за въздействие може да се отнася за повече от един проект.

(2) При извършване на ОВЗД администраторът изисква становището на ДЛЗД.

Раздел II
Оценка на риска при обработката на лични данни

Чл. 5. (1) Всички дейности, осъществявани от МФ, които предвиждат обработка на лични данни, са предмет на предварителна оценка на риска.

(2) Всяко от административните звена в МФ, което обработва лични данни, идентифицира рисковете, свързани със защитата на лични данни, за което попълва риск-регистър (*Приложение № 11*), в който се анализира вероятността за възникване на нарушение на сигурността на данните както и възможното влияние при евентуалното им възникване. При оценката на риска се определят 3 нива на риска – нисък (приемлив), среден (изисква внимание), висок (неприемлив). Оценката на риска се извършва най-малко веднъж годишно и се ръководи от ДЛЗД в МФ.

Чл. 6. При определянето на степента на риска администраторът трябва да вземе предвид:

1. критериите за вероятен „висок риск“ на чл. 35, § 3 от ОРЗД;
2. общите положения на Стратегията за управление на риска в МФ;
3. съответните рискови области (стратегически рискове, оперативни рискове, политически рискове, икономически рискове, рискове за репутацията, правни/регулатиорни рискове, рискове за сигурността и т.н.);
4. всички отношения на МФ с външни субекти (други организации, контрагенти по договори, граждани и др.).

Чл. 7. (1) В зависимост от определеното ниво на въздействие администраторът извършва:

1. приоритизация на идентифицираните рискове в зависимост от резултатите от оценката им.
2. определяне на стойността и рейтинга на всеки риск;
3. определяне на адекватно ниво на защита, включващо техническите и организационни мерки, които трябва да предприеме за тяхното ограничаване.

(2) В зависимост от приоритизацията на рисковете и идентифицираното ниво на въздействие се определя съответно ниво на защита – ниско, средно или високо, както и организационните и технически мерки, адекватни на така определеното ниво.

Раздел III
Предварителни консултации с надзорния орган

Чл. 8. (1) Задължителна предварителна консултация с надзорния орган е необходима, когато:

1. оценката на въздействието върху защитата на данните покаже, че предвиденото обработване ще породи висок риск и;
2. администраторът не може да предприеме ефективни мерки за ограничаването му.

(2) Предварителна консултация може да не бъде проведена, ако администраторът счита, че идентифицираният риск може да бъде смекчен с разумни средства по отношение на наличните технологии и разходите за изпълнение.

ГЛАВА III
ОРГАНИЗАЦИОННИ И ТЕХНИЧЕСКИ МЕРКИ ЗА ЗАЩИТА НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ В МФ

Раздел IV
Организационни мерки

Чл. 9. (1) За защита на сигурността на личните данни администраторът:

1. със своя заповед определя длъжностно лице по защита на данните в МФ;
2. извършва оценка на въздействието върху защитата на данните;
3. задължава всички служители, които обработват лични данни да спазват

изискванията за поверителност на личните данни, до които имат достъп, съгласно правилата на ОРЗД, настоящата Политика и отговорностите на МФ като администратор на лични данни.

(2) Администраторът организира обучение на персонала за обработване на лични и чувствителни лични данни и за извършване на оценка на въздействието върху защитата на данните в отделните административни звена на МФ.

(3) При оценяването на подходящите организационни мерки ДЛЗД взема предвид следното:

1. нивата на подходящо обучение на служителите в Министерството на финансите;
2. идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
3. редовна проверка на персонала за спазване на съответните стандарти за сигурност;
4. контрол на физическия достъп до електронни и хартиено базирани записи;
5. спазване на правилото за „чисто работно място“;
6. начина на съхраняване на данните от служителите;
7. ограничаване на използването от служителите на лични устройства на работното място.

Чл. 10. (1) МФ изисква гаранции от трети лица - обработващи лични данни, че са в състояние да осигурят необходимата защита на личните данни.

(2) При влизане в договорни отношения с обработващите лични данни се включват договорни клаузи, според които обработващите лични данни трябва да гарантират, че предоставят достатъчни технически и организационни мерки за защита на сигурността и поверителността на личните данни и ще действат според указанията на администратора.

Раздел V
Технически мерки

Чл. 11. (1) Техническите мерки за защита на лични или чувствителни лични данни включват:

1. класифициране на данни;
2. предотвратяване на загуба на данни;
3. криптиране;
4. получаване на изрично съгласие за всяка конкретна цел;
5. ограничения при пренос на данни и въвеждане на технологии, които позволяват на субектите на данни да упражняват своите права за достъп;
6. коригиране и заличаване на лични данни;
7. начини на защита с парола;
8. автоматично заключване при неизползване на работните станции в мрежата;
9. премахване/ограничаване на права на достъп за USB и други преносими носители с памет;
10. антивирусен софтуер и защитни стени за блокиране на зловреден софтуер;
11. защитата на преносими устройства, които напускат помещенията на организацията, като лаптопи и други;
12. осигуряване сигурността на локалните и широкообхватните мрежи;
13. осигуряване на технологии за подобряване на поверителността – псевдонимизиране или анонимизиране;
14. внедряване на подходящи услуги за съхранение и споделяне на облак, които активно блокират или обезкуражават използването на неоторизирани услуги и отговарят на правата за достъп, коригиране и заличаване на субектите на данни, определени от ОРЗД;
15. активно наблюдение на действията за споделяне, за да се сведе до минимум вероятността от нарушаване на данните.

(2) Всички служители, оправомощени да обработват лични данни, са длъжни да спазват следните мерки за защита на данните:

1. на хартиен носител:

а) личните данни на хартиен носител се съхраняват в специални помещения, или заключена каса/шкаф, в зависимост от вида на данните, при спазване на специални мерки за достъп до помещението;

б) когато личните данни трябва да бъдат прехвърлени на хартиен носител, те трябва да бъдат предадени директно на получателя срещу подпис или изпратени с препоръчана поща с обратна разписка;

в) когато някоя лична информация трябва да бъде заличена по някаква причина (включително когато са направени копия, които вече не са необходими), тя се унищожава като се нарязва на шредер машина, след което се изхвърля;

2. на електронен носител – съгласно правила, определени в Политиката по мрежова и информационна сигурност на информационни системи в МФ и съпътстващите я документи, утвърдени от министъра на финансите, главния секретар и директора на дирекция ИС. Набелязаните технически мерки се прилагат и за защита на личните данни.

Чл. 12. Неспазването на техническите и организационни мерки за защита на данните и останалите вътрешни актове, свързани със защита на данните, е основание за търсене на дисциплинарна отговорност от виновните служители.

Раздел VI
Документиране на дейностите по обработване. Регистър на обработванията на данни

Чл. 13. (1) В МФ се поддържа Регистър на дейностите по обработванията на данни, достъпът до който се осъществява съгласно функционален принцип.

(2) Регистърът по ал. 1 съдържа следната информация:

1. името и координатите за връзка на администратора и ДЛЗД;
2. целите на обработването;
3. описание на категориите субекти на данни и на категориите лични данни;
4. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
5. когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея, документация за подходящите гаранции;
6. предвидените срокове за изтриване на различните категории данни;
7. общо описание на техническите и организационни мерки за сигурност.

(3) Регистърът по ал. 1 се подържа чрез платформата Апис „GDPR Асистент“, а вписването в него се извършва от ДЛЗД.

(4) При нововъзникнала дейност по обработка на лични данни административното звено, което извършва обработването, следва да уведоми ДЛЗД като представи необходимата информация по ал. 2.

Чл. 14. Служителите на администратора, които обработват лични данни от негово име, осигуряват сигурността при обработването и съхраняването на данните от тяхна страна, включително гарантират, че няма да разкриват данните на трети страни, освен ако администраторът не е дал такива права на тази трета страна за достъп до данните.

Чл. 15. При обработката на данни чрез видеонаблюдение, при което се извършва запис чрез технически средства за видеонаблюдение, се спазват Правилата за извършване на видеонаблюдение в обектите на администратора (*Приложение № 3.*).

Раздел VII
Профилиране

Чл. 16. (1) Профилирането е автоматизирано обработване на лични данни с цел оценяване на определени лични аспекти, свързани с дадено лице, включително за анализиране или прогнозиране на поведението му, изпълнение на професионалните му задължения, икономическото му състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.

(2) В случай, че администраторът използва лични данни за целите на профилирането, следва да са изпълнени следните условия:

1. да бъде предоставена ясна информация, поясняваща профилирането, включително значението и вероятните последици;

2. да се използват подходящи статистически или математически процедури;

3. да се въведат технически и организационни мерки, необходими за минимизиране на риска от грешки, за да се позволи лесното им отстраняване и да се предотврати дискриминационното въздействие.

Раздел VIII
Разкриване на данни

Чл. 17. (1) Личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, ако има основателно съмнение, че не се изискват по установения ред. Всички служители трябва да следят дали искането от трета страна за разкриване на лични данни за друго лице е свързано или не с нуждите на дейността, извършвана от администратора.

(2) Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат координирани с ДЛЗД, което да даде становище.

(3) В качеството си на орган по назначаването министърът на финансите предоставя лични данни на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служителите и/или изпълнители по граждански договори. В тези случаи личните данни включват трите имена и единен граждански номер и служат за идентификация на лицето, в чиято полза се извършва плащането.

(4) Във връзка с използването на куриерски услуги – приемане, пренасяне, доставка и адресиране на пратки до физически лица, МФ посочва следните данни: две имена, адрес, област, наименование на населеното място с пощенски код.

(5) Личните данни се предоставят на компетентните органи при и по повод упражняване на техните властнически правомощия.

Раздел IX
Преносимост

Чл. 18. (1) МФ отговаря за прехвърлянето на данните без затруднения и гарантира, че те се предават със съответното ниво на комуникационна сигурност.

(2) Субектите на данни имат право да поискат:

1. копие от личните данни, които са предоставили на МФ;

2. МФ да прехвърли тези данни на друг администратор посочен от субекта, без възпрепятстване.

(3) Преносимост се прилага само за тези данни, за които:

1. субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

2. обработването им е било 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 им е било извършено по автоматизиран начин;

4. МФ е получило информация за субекта на данни от друг администратор, който е решил да упражни правото си на преносимост, като в тези случаи МФ се явява администратор по отношение на новоприетите данни.

Чл. 19. (1) МФ приема и съхранява само данните, които са необходими и относими към определена дейност. МФ не приема и не обработва лични данни „по подразбиране“, дори когато са получени от друг администратор след искане за прехвърлянето им, както и не съхранява всички получени данни.

(2) Ако получените данни съдържат данни за трети лица, МФ съхранява данните под контрола на субекта заявител. Тези данни се обработват само за определената цел.

Чл. 20. При постъпване на искане за предаване или за прехвърляне на лични данни към друг администратор МФ обработва искането на субекта при спазване на следните правила:

1. всяко постъпило искане незабавно се изпраща на ДЛЗД, което проверява за ясни и неоспорими доказателства за самоличността на субекта на данни под формата на лични документи, клиентски номер, електронна карта или друг еднозначен идентификатор;

2. ДЛЗД проверява дали посочените от субекта данни са получени на основание съгласие, изпълнение на законово правомощие или функция, или договор и дали са обработени по автоматизиран начин. Ако не са изпълнени тези изисквания, МФ има право да откаже да удовлетвори искането;

3. когато исканите данни засягат трето лице/а, ДЛЗД преценява дали предаването на данни на друг администратор на лични данни би навредило на правата и свободите на други субекти на данни;

4. ДЛЗД извършва проверка дали подготвените за предаване/прехвърляне лични данни са само и точно тези, които субектът на данни е поискал да бъдат предадени, респ. прехвърлени;

5. поисканата информация се предоставя на субекта на данни в структуриран, широко използван и машинно четим формат, който позволява ефективно повторно използване на данните;

6. при предаване на данните на друг администратор на данни МФ ги препраща в оперативно съвместим формат. В случай, че са налице технически пречки, които възпрепятстват директното им прехвърляне, МФ съобщава тези пречки на субекта на данните;

7. МФ предоставя исканата информация в рамките на един месец от датата на заявката. Ако заявката е сложна, МФ може да удължи тази времева рамка максимум до три месеца от датата на предявяването ѝ. МФ информира субекта на данни за причините за забавянето чрез имейл, телефон и др. в рамките на един месец от първоначалното искане;

8. ДЛЗД поддържа записи за исканията за прехвърляне на данни в Регистъра на исканията, включително всички, свързани с преносимостта дати.

Раздел X
Съхраняване и унищожаване на лични данни

Чл. 21. При съхранение на лични данни МФ:

1. прилага основния принцип за съхранение на лични данни в минимален обем и за срок не по-дълъг от необходимото или определеното от закона за съответните категории данни;

2. осигурява тяхната сигурност и надеждност и изискванията на съответния закон;

3. заличава личните данни след изтичането на съответния срок;

4. може да запази лични данни за по-дълъг от съответния срок – до окончателното приключване на възникнал правен спор или производство, налагащо запазване на данни, и/или по искане на компетентен орган.

Чл. 22. (1) Лични данни в МФ се съхраняват при спазване на Вътрешните правила за организацията на хартиения и електронния документооборот и контрола по изпълнение на задачите в МФ и се унищожават при спазване на Вътрешните правила за организацията и дейността на учрежденския архив на МФ:

1. по искане на субекта на лични данни, когато то е прието за основателно;

2. по предложение на ръководителите на административни звена, в които се събират или обработват лични данни, когато се прецени, че е отпаднала нуждата от обработване и съхранение.

(2) При унищожаване на лични данни МФ:

1. всяка календарна година със заповед на министъра на финансите се определя състав

на комисия, която да извършва анализ на личните данни в МФ от гледна точка на сроковете за съхраняването им.

2. в състава на комисията се включва поне един представител от административните звена, които събират и обработват лични данни.

3. при необходимост от унищожаването на лични данни се изготвя предложение до министъра на финансите, което се съгласува с ДЗЛД и ръководителите на административни звена, в които се събират или обработват лични данни.

4. след резолюция на министъра на финансите, личните данни се унищожават като се изготвя протокол, който съдържа:

а) вида на личните данни;

б) водещото административно звено, в което са обработвани или съхранявани личните данни;

в) вида на обработката на лични данни (за какво са събрани и обработвани);

г) броя на унищожените записи с лични данни;

д) трите имена на субектите с унищожени лични данни.

(3) Унищожаването на данни се извършва по следните начини:

1. при данни на хартиен носител – чрез нарязване в специални машини за унищожаване на документи, в които се унищожат както оригиналните документи, така и копията към тях;

2. при данни на електронните носители – чрез изтриване както в системата, в която се съхраняват или мястото им файловия сървър на МФ, така и в архивните копия, които са направени от дирекция „Информационни системи“.

(4) След изготвяне от комисията протокола се представя на министъра на финансите за утвърждаване и се предава на ДЛЗД за съхранение.

ГЛАВА IV
ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИ

Чл. 23. Длъжностното лице по защита на данни се определя със заповед на министъра на финансите и има следните отговорности:

1. изпълнява задачи, свързани със защита на личните данни, съобразно настоящата Политика;

2. взема участие на заседанията на ръководството на администратора, на които се обсъждат въпроси от областта на защита на личните данни и съветва администратора за доказване на съответствието със законодателството в областта на защита на данните и добрите практики;

3. наблюдава спазването на ОРЗД и на други разпоредби за защитата на данни на равнище ЕС или държава членка и на политиките на администратора по отношение на защитата на личните данни. При констатирани несъответствия докладва на министъра на финансите, като прави предложения за подобряване на процедурите по отношение на защита на личните данни в МФ;

4. поддържа Регистър на дейностите по обработванията на данни, Регистър на исканията от субекти на данните, Регистър на инцидентите;

5. сътрудничи с Комисията за защита на личните данни и действа като точка за контакт по всички въпроси, свързани с обработването на лични данни;

6. оказва съдействие по въпроси, свързани с упражняването на правата по защита на лични данни;

7. отчита се пряко пред министъра на финансите.

ГЛАВА V
ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Чл. 24. **(1)** Всички външни изпълнители и техни подизпълнители, които обработват лични данни от името на администратора, са обработващи лични данни по смисъла на ОРЗД.

(2) МФ избира само външни изпълнители, които могат да осигурят техническа, физическа и организационна сигурност и които отговарят на поставените изисквания по отношение на всички лични данни, които ще обработват. При прекратяването на договор с изпълнител/подизпълнител съответните лични данни трябва да бъдат унищожени или върнати на МФ.

(3) Когато МФ разреши на външния изпълнител да превъзложи обработката на лични данни на подизпълнител, външният изпълнител трябва да забрани на подизпълнителя (и следващите подизпълнители, ако има такива) да превъзлага дейността по обработка на данни на подизпълнители без писменото разрешение на МФ.

(4) МФ има право да извършва редовни проверки на системите за сигурност на външния изпълнител през периода, в който той има достъп до личните данни.

(5) Административното звено в МФ, което осъществява текущ контрол и приема резултатите от изпълнението на договор, редовно извършва преглед на съответния договор, за да провери дали се обработват лични данни. Тези проверки се извършват, дори ако дейността по обработка на лични данни не е основната причина за сключване на договора.

Чл. 25. Изпълнители от страни извън ЕС могат да бъдат избрани само при положение, че е изпълнено поне едно от следните специфични условия:

1. ако изпълнителят или държавата, в която пребивава или е установен, са били идентифицирани като осигуряващи адекватно ниво на защита на личните данни в решение за адекватност от страна на Европейската комисия;
2. ако са налични задължителни фирмени правила за предаване на данни извън ЕС, за да се гарантират правата на субектите, и тези правила са одобрени от Комисията за защита на личните данни;
3. когато споразумението с изпълнителя е одобрено от надзорния орган.

ГЛАВА VI
ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл. 26. **(1)** Субектът на лични данни има следните права по отношение на обработването на личните му данни:

1. да получи информация за личните данни, свързани с него, които се обработват от администратора, и за целта, за която се обработват, включително да получи достъп до данните в структуриран, широко използван и пригоден за машинно четене формат, както и информация кои са получателите на тези данни и третите страни, на които данните се предават;
2. да иска от администратора коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;
3. да изиска от администратора изтриване на лични данни (право „да бъдеш забравен“);
4. да иска от администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани;
5. да направи възражение срещу обработване на негови лични данни. Жалби могат да се подават и направо до надзорния орган, компетентен за България – Комисията за защита на личните данни, адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2 (www.cpdp.bg);
6. да се обърне с жалба до надзорен орган, ако смята, че някоя от разпоредбите на ОРЗД е нарушена;
7. да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора (*Приложение № 5)*;
8. да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса.

(2) Субектът на лични данни може да отправи искане до администратора, в което указва вида на искането и описание на данните съгласно образец *(Приложение № 4)*. В искането задължително се посочва самоличността на субекта, която да го идентифицира сигурно и еднозначно (данни от лични документи, клиентски номер, електронна идентификационна карта и т.н).

(3) Министерството на финансите документира и доказва, че субектът на данните е оттеглил съгласието си за обработката на личните му данни, а когато обработката има множество цели, МФ документира и доказва оттеглянето на съгласието за всяка отделна цел.

Чл. 27. Министерството на финансите осигурява условия, които да гарантират упражняването на правата по предходния член от субектите на лични данни, като:

1. задължително проверява идентификационните данни, за да се увери, че искането е подадено от субекта, който данните идентифицират;
2. документира датата на получаване на искането;
3. произнася се по искането;
4. изпраща отговор на подателя, в който го информира за правото на жалба до Комисията за защита на личните данни, като едновременно с това предоставя координатите за контакт и правото за защита по съдебен ред.

Чл. 28. (1) Подаването на искания, оплаквания и жалби може да се извърши и чрез електронна поща, контролирана и проверявана от ДЛЗД, в случай, че документът е подписан с електронен подпис и може да идентифицира субекта на лични данни. В този случай всички приложения към искането следва да са представени в електронен вид и заверени с електронен подпис.

(2) В случай, че искането от субект на данни не бъде получено от ДЛЗД, то незабавно му се препраща за:

1. вписване в Регистъра на исканията от субекти на данните;
2. обработка чрез идентифициране (търсене) на личните данни във всички хранилища на данни и всички съответни системи за архивиране, включително всички архивирани файлове (автоматични или ръчни архиви) и всички папки на електронната поща и техните архиви лично или чрез съответните административни звена в МФ, които обработват данните;
3. обработване на данните с цел отстраняване на евентуална идентификационна информация за трети лица при предаването на копие от информацията, когато искането е за достъп до информация;
4. изготвяне на проект на отговор от името на администратора до субекта на данните най-късно на един месец от датата на получаване на искането за достъп;
5. вписване в Регистъра на исканията данни за подадения отговор.

(3) При искания на субекти на данни за коригиране, изтриване, ограничаване или при възражение по отношение на обработваните лични данни, които са приети са основателни, ДЛЗД следи за изпълнението на взетото решение като:

1. участва в документирането по премахване на личните данни от системите и прекратяване на операциите по обработката им;

2. участва в документирането за всяко извършено коригиране, изтриване или ограничаване на обработването на всеки получател, на когото личните данни са били разкрити.

(4) Когато исканията на субекти на данни са явно неоснователни или прекомерни поради своята повторяемост, ДЛЗД може мотивирано да предложи на администратора:

1. да откаже да предприеме действия по искането като изложи причините за непредприемане на действията или отказа;
2. да наложи разумна такса, предвид административните разходи за предоставяне на информацията или комуникацията и да разгледа искането.

Чл. 29. Субектите на данни могат да подадат до МФ и:

1. оплаквания относно на начина на разглеждане на искането им за достъп до данните;
2. оплаквания относно начина на разглеждане на искането/жалбата им;
3. жалба срещу всяко решение, взето след подадено искане/жалба.

Чл. 30. Ограничения на правата на субектите са допустими с цел да се гарантира:

1. националната сигурност и отбраната;
2. обществената сигурност;
3. предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;

4. важни цели от широк обществен интерес;

5. важен икономически или финансов интерес на ЕС или на държава-членка, паричните, бюджетните и данъчните въпроси;

6. общественото здраве и социалната сигурност;

7. защитата на независимостта на съдебната власт и съдебните производства;

8. предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;

9. функция по наблюдението, проверката или регламентирането, свързана с упражняването на официални правомощия в определени от закон случаи;

10. защитата на субекта на данните или на правата и свободите на други лица;

11. изпълнението по гражданскоправни искове.

ГЛАВА VII
ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 31. (1) Администраторът обработва специални категории лични данни, когато това произтича от закон.

(2) Условията за обработване на специални данни са:

1. получаване на изрично писмено съгласие от субекта на данни (*Приложение № 2*) за една или повече конкретни цели, освен когато законодателството на ЕС или националното законодателство предвижда, че забраната не може да бъде отменена от субекта на данните. Съгласието трябва да бъде дадено свободно, конкретно, информирано и недвусмислено и се ограничава само до обработването за целите, за които е дадено;

2. обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото и осигурителното право;

3. обработването е необходимо за защита на жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните физически или юридически не е в състояние да даде съгласието си;

4. обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

5. обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи;

6. обработването е необходимо по причини от важен обществен интерес на основание правото на ЕС или националното законодателство, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;

7. обработването е необходимо за целите на превантивната или трудовата медицина;

8. обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно чл. 89, параграф 1 от ОРЗД, на основание правото на ЕС или националното законодателство.

Чл. 32. (1) Получаване на съгласие от дете се изисква, когато обработката на лични данни е свързана с дете на възраст под 16 години, а лицето, което носи родителска отговорност за детето, е предоставило съгласието си съгласно образец на форма за съгласие от родител/настойник (*Приложение № 6*).

(2) Оттегляне на съгласие от родителите на дете се извършва от лицето, което носи родителската отговорност за посоченото дете, съгласно форма за оттегляне на съгласие от родител/настойник *(Приложение № 7).*

(3) МФ доказва, че са направени разумни усилия, за да се установи автентичността на родителската отговорност от носещия родителската отговорност при даване и оттегляне на съгласието за определено дете.

ГЛАВА VIII
НАРУШЕНИЯ НА СИГУРНОСТТА НА ДАННИТЕ. СРЕДСТВА ЗА ПРАВНА ЗАЩИТА СРЕЩУ НАРУШЕНИЯ

Чл. 33. **(1)** Всички служители са длъжни да докладват на ДЛЗД за всяко нарушение на сигурността на личните данни, което е вероятно да породи риск за правата и свободите на физическите лица, свързано с нарушаване на:

1. поверителността – когато има неразрешено или случайно разкриване на, или достъп до лични данни;
2. достъпността/наличността – при случайна или неразрешена загуба на достъп до или унищожаване на лични данни;
3. интегритета – когато има неразрешено или случайно изменение на личните данни.

(2) При докладвано нарушение ДЛЗД предприема незабавни действия по действителното му установяване и анализ на възможните последици за отделните лица.

Чл. 34. **(1)** ДЛЗД изготвя уведомление за нарушение на сигурността на личните данни (*Приложение № 8)* до Комисията за защита на личните данни без ненужно забавяне и не по-късно от 72 часа, след като е узнал за нарушението. При необходимост от провеждане на допълнителна проверка е необходимо получаване на съгласие от надзорния орган за срока и начина на предоставяне на допълнителната информация.

(2) ДЛЗД изготвя уведомление за нарушение на сигурността на личните данни (*Приложение № 9*) до субекта на данни, който разполага със средствата за защита и може да търси отговорност за причинените му вреди по реда на Закона за защита на личните данни.

(3) В случаите на установяване на нарушение на сигурността на личните данни от обработващ, същият подава уведомление до администратора на лични данни за нарушение на сигурността (*Приложение № 10*), в което описва естеството на нарушението, засегнатите данни и субекти, последиците от нарушението, предприетите технически и организационни мерки и изисква от администратора да посочи евентуални допълнителни мерки за сигурност.

(4) ДЛЗД документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него, като води отделен регистър, в който задължително се вписват:

1. предполагаемото време или период на възникване;
2. времето на установяване;
3. времето на докладване и името на служителя, извършил доклада;
4. последствията от инцидента и
5. мерките, които са предприети за отстраняването им.