ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ДЪРЖАВНАТА АГЕНЦИЯ ЗА БЕЖАНЦИТЕ ПРИ МИНИСТЕРСКИЯ СЪВЕТ

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Тези Вътрешни правила уреждат условията и реда за обработване на лични данни, водене на регистри на лични данни, технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни в Държавната агенция за бежанците при Министерския съвет (ДАБ при МС).

Чл. 2 Вътрешните правила имат за цел да регламентират:

2.1 индивидуализиране на администратора на лични данни;

2.2 общо описание на поддържаните регистри-категории лични данни и основание за обработване;

2.3 технологично описание на поддържаните регистри-носители на данни, технология за обработване, срок за съхранение и предоставени услуги;

2.4 определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им;

2.5 оценка на въздействие и определяне на съответно ниво на защита и организационни мерки и допустимия вид защита на личните данни;

2.6 описание на предприетите технически и организационни мерки за защита на личните данни;

2.7 действия за защита при аварии, произшествия и бедствия (пожар, наводнение и тн.);

2.8 предоставяне на лични данни на трети лица-основание, цел, категории лични данни;

2.9 срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.

Принципи при обработване на лични данни

Чл. 3 (1) При обработването на лични данни в ДАБ при МС се спазват следните принципи:

1.Законосъобразност, добросъвестност и прозрачност- обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни.

а) обработването е необходимо за изпълнение на определено правно задължение;

б) обработването е необходимо за изпълнение на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

в) обработването е основано на доброволно и информирано съгласие на субекта на данните;

г) в случаите, когато се обработват данни на деца под 14-годишна възраст, това обработване е законосъобразно, само ако и доколкото такова съгласие е дадено от родител или настойник на детето;

д) ДАБ при МС осигурява възможност на субекта на данни по всяко време да оттегли своето съгласие за обработване на данни, като подаде декларация за оттегляне на съгласие.

е) За постигане на конкретно определени цели ДАБ при МС обработва и специални категории лични данни.

д) Обработването на лични данни по ал. 3, буква „е“ се извършва само в случаите, когато субектът на данни е дал своето изрично съгласие за обработването им и същото е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните, доколкото това е разрешено от правото на ЕС или националното законодателство, в което се предвиждат подходящи гаранции за основните права и интереси на субекта на данните.

(2) Ограничение на целите- събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

(3) Свеждане на данните до минимум-данните да са подходящи, свързани със и ограничени до необходимото във връзка със 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 на лични данни носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Условия за достъп до лични данни

Чл. 4 (1) Достъпът до лични данни в ДАБ при МС се осъществява при прилагане на принципа „Необходимост да знае“.

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

а) които обработват данни в изпълнение на служебните/трудовите си задължения съгласно акта за назначаване и/или сключения трудов договор и длъжностната характеристика за съответната длъжност;

б) които са оторизирани с изричен акт на Председателя на ДАБ при МС;

в) които изпълняват сключени с ДАБ при МС договори;

(3) Достъп до лични данни се предоставя след запознаване на лицата с нормативната уредба в областта на защитата на личните данни, настоящите правила и процедури за защита на личните данни на администратора, което се осъществява от Длъжностното лице по защита на личните данни.

(4) Оторизираните с право на достъп лица подписват Декларация за конфиденциалност на личните данни, до които получават достъп при и по повод изпълнение на задълженията си, както и за преминалото обучение по ал. 3.

(5) Декларацията по ал. 4 се предоставя на лицата от Дирекция „Административно-правно обслужване и човешки ресурси“ при тяхното назначаване и се прилага към служебно/трудово досие.

(6) ДАБ при МС осигурява възможност на субекта на данни по всяко време да оттегли своето съгласие за обработване на данни, като подаде декларация за оттегляне на съгласие.

(7) Лицата, които имат достъп до лични данни носят отговорност за опазване на носителите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни може да бъде основание за налагане на дисциплинарни или гражданскоправни санкции, а в определени случаи и наказателна отговорност.

Права на физическите лица при обработване на отнасящи се за тях лични данни

Чл. 5 (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

5.1 данните, които идентифицират администратора;

5.2 целите на обработването на личните данни и правното основание за обработването;

5.3 категориите лични данни, отнасящи се до съответното физическо лице;

5.4 получателите или категориите получатели, на които могат да бъдат разкрити данните;

5.5 срока за съхранение на личните данни;

5.6 информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на

преносимост при условията на Регламент (ЕС) 2016/679-Общия регламент относно защитата на личните данни;

5.7 право на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

5.8 правото на жалба до надзорен орган- Комисията за защита на личните данни;

5.9 източника на данните;

(2) Алинея 1 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

2. вписването или разкриването на данни са изрично предвидени в закон;

3. е налице изрична забрана за това в закон;

(3) Информацията по ал. 1 се обявява на леснодостъпно място на електронната страница на ДАБ при МС.

II. АДМИНИСТРАТОР НА ДАННИТЕ И ДЛЪЖНОСТНО ЛИЦА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Индивидуализация на администратора на лични данни

Чл. 6 (1) Администратор на лични данни е ДАБ при МС, със седалище и адрес на управление: гр. София, бул. „Княгиня Мария Луиза“ № 114Б. Адресът за кореспонденция и контакт е гр. София, бул. „Княгиня Мария Луиза“ № 114Б, работно време: понеделник-петък, 08:30-17:00 ч., електронна поща: sar@saref.government.bg

(2) ДАБ при МС обработва лични данни във връзка с изпълнението на законовите си правомощия, като определя целите и средствата за обработването им, при спазване на относимите нормативни актове.

(3) Личните данни се обработват самостоятелно от администратора на лични данни и чрез възлагане на обработващи лични данни.

Длъжностно лице по защита на личните данни

Чл. 7 Длъжностното лице по защита на личните данни се определя със Заповед на Председателя на ДАБ при МС.

Чл. 8 За длъжностно лице по защита на личните данни може да бъде определен и служител, който да съвместява с друга длъжност.

Чл. 9 Данните за контакт с длъжностното лице по защита на личните данни се публикуват на интернет страницата на ДАБ при МС https://aref.government.bg

Чл. 10 Длъжностното лице по защита на личните данни се отчита пряко пред администратора на лични данни (Председателя на ДАБ при МС) и има следните задължения и отговорности:

10.1 Да предоставя съвети по отношение на оценката на въздействието върху защитата на лични данни;

10.2 Да информира и консултира/съветва администратора на лични данни-Председателя на ДАБ при МС;

10.3 Да наблюдава спазването на нормативните изисквания в областта на личните данни, включително повишаването на осведомеността и обучението на персонала;

10.4 Да спазва конфиденциалността на изпълняваните задачи;

10.5 Да си сътрудничи с Комисия за защита на личните данни;

10.6 Да действа като точка за контакт с Комисия за защита на личните данни;

10.7 Да води регистър на дейностите по обработване на личните данни;

10.8 Да подпомага администратора, като своевременно уведомява Комисията за защита на личните данни, в срок от 72 часа от узнаване на нарушението на сигурността на личните данни;

10.9 Да участва при изготвянето на вътрешни правила и документи, свързани със защита на личните данни, както и да организира и да предлага при необходимост актуализиране на декларациите или други форми за документиране дейността по защита на личните данни.

Чл. 11 Длъжностното лице по защита на личните данни е независимо и не получава указания или разпореждания, във връзка с изпълнение на своите задачи по защита на личните данни.

III. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 12 (1) ДАБ при МС, в качеството си на администратор на лични данни, води и поддържа следните регистри на дейностите по обработване на лични данни:

12.1 Регистър „Чужденци, подали молба за закрила“;

12.2 Регистър „АИС Бежанци“;

12.3 Регистър „Управление на човешките ресурси“;

12.4 Регистър на доставчиците, изпълнители по договори;

12.5 Регистър „Възнаграждения и други плащания на персонала“;

12.6 Регистър на академичния състав във висшите училища;

12.7 Регистър „Обществени поръчки“;

12.8 Регистър „Чужденци с изготвен интеграционен профил“;

12.9 Регистър на декларациите по чл. 49, ал. 1 от Закона за противодействие на корупцията;

12.10 Регистър „Видеонаблюдение“.

(2) Данните от регистрите по ал. 1 се обработват от служители/работници на ДАБ при МС при спазване на принципа „Необходимост да се знае“.

(3) Работниците/служителите на ДАБ при МС нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните/трудовите им задължения.

(4) Отговорност за създаването и поддържането на регистрите в актуален вид носят ръководителите на организационните звена, които извършват дейности по обработка на личните данни.

Чл. 13 (1) В регистър „Чужденци, подали молба за закрила“ се обработват лични данни на чужденци, подали молба за международна закрила, с оглед ползване на информацията в областта на предоставяне на закрила, както следва:

1. данни относно физическата идентичност на чужденците: имена, дата и място на раждане, националност, гражданство, ЛНЧ, национални документи, дактилоскопен лист, описание на лицето (ръст и особени белези), снимков материал, подпис, адрес, телефон за връзка и др.

2. образование;

3. етническа и религиозна принадлежност;

4. семейно положение;

5. здравен статус на кандидата за закрила;

6. политически и религиозни убеждения и членство в политически партии;

(2) Личните данни се събират от чужденци, търсещи международна закрила въз основа на правото на ЕС в областта на предоставяне на международна закрила, Закона за убежището и бежанците (ЗУБ) и всички законови и подзаконови нормативни актове, приложими към тази дейност.

(3) Регистър „Чужденци, подали молба за закрила“ се води на хартиен и на технически носител.

(4) В случаите, когато регистър „Чужденци, подали молба за закрила“ се води и на хартиен носител, се спазват следните правила:

1. данните се набират на хартиен носител и се съхраняват в лични досиета на чужденците в ДАБ при МС;

2. личните досиета до приключване на производството с влязло в сила решение се съхраняват в центровете, където се провежда производството;

3. работниците/служителите, оператори на лични данни, обработващи личните данни от името на администратора, предприемат организационно-технически мерки за съхраняването и опазването на личните досиета, в т.ч. и ограничаване на достъпа до тях на външни лица;

4. личните досиета на чужденците в ДАБ при МС не се изнасят извън сградата на администратора;

5. след приключване на производството личните досиета се предават с протокол на дирекция „Качество на процедурата за международна закрила“ (КПМЗ), като същите се съхраняват в обособено помещение, защитено със съответните технически средства (метална врата, решетки на прозорците и система за пожароизвестяване). Достъп до помещението имат работникът/служителят, отговарящ за архива, работникът/служителят, определен да го замества в негово отсъствие и директорът на дирекция КПМЗ в присъствието на работника/служителя, отговарящ за архива;

6. справки и ползване на архивирани лични дела се правят чрез попълване на искане (по образец) и след подписване на искането от директора на дирекция КПМЗ;

7. личните дела, изискани от териториалните поделения, се изпращат с приемо-предавателен протокол;

8. работникът/служителят, отговарящ за архива, записва в регистър номера на искането лично дело, датата на предаване, имената на работника/служителя, получил делото и номера и датата на искането.

(5) В случаите, когато регистър „Чужденци, подали молба за закрила“ , се води на технически носител, се спазват следните правила:

1. личните данни се въвеждат (в база данни и отделни файлове) на компютрите на оператора на лични данни, свързани в локална мрежа, със защитен достъп до личните данни;

2. достъп имат само операторите на лични данни;

3. компютрите са изолирани в помещения за самостоятелна работа;

4. достъп до организационната система, съдържаща файлове за обработка на лични данни, имат само обработващите лични данни чрез индивидуална парола;

5. защитата на електронните данни от неправомерен достъп се осигурява чрез поддържане на антивирусни програми, както и автоматизирано архивиране на данните на външно устройство, свързано с база данни.

(6) Личните данни се обработват от работници/служители в дирекция КПМЗ и териториалните поделения.

(7) По време на производството в ДАБ при МС и шест месеца след влизане в сила на решението, личните дела на чужденците се съхраняват в съответното териториално поделение, в което се провежда производството. След изтичане на този срок, комплектуваните в цялост лични дела се изпращат за архив в дирекция КПМЗ. В помещенията, където се архивират делата, имат право на достъп работникът/служителят, отговарящ за архива, работникът/служителят, определен да го замества и директорът на дирекция КПМЗ в присъствието на работника/служителя, отговарящ за архива. При необходимост други лица, извън посочените, могат да бъдат допуснати в архива само в присъствието на работника/служителя, отговарящ за архива или работника/служителя, определен да го замества.

(8) Директорът на териториалното поделение определя работник/служител, който да организира съхраняването на личните дела.

(9) Административните преписки се съхраняват 20 години в централния архив към дирекция КПМЗ.

(10) Оценка на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 14 (1) В регистър „АИС Бежанци“ се обработват лични данни на чужденци, търсещи международна закрила, както следва:

1. имена, дата и място на раждане, националност, гражданство, ЛНЧ, национални документи, дактилоскопен лист, описание на лицето (ръст и особени белези), снимков материал, подпис, адрес, телефон за връзка и тн.;

2. образование;

3. етническа и религиозна принадлежност;

4. семейно положение;

5. здравен статус на кандидата за закрила;

6. политически и религиозни убеждения;

7. процесуален съдебен статус.

(2) Личните данни се обработват от работници/служители в дирекция КПМЗ и териториалните поделения.

Чл. 15 (1) В регистър „Управление на човешките ресурси“ се обработват лични данни на работници/служители в ДАБ при МС, както следва:

1. физическа идентичност-имена, ЕГН, адрес, телефон, електронна поща;

2. социална идентичност-образование, трудова дейност, квалификация;

3. медицинско свидетелство и свидетелство за съдимост при започване на работа;

4. семейно положение;

5. здравен статус на работниците/служителите;

6. данни за номера на банкова сметка с оглед изплащане на служебни и трудови възнаграждения и обезщетения.

(2) Обработката и съхранението на лични данни в регистър „Управление на човешките ресурси“ се извършва при и по повод изпълнение на нормативните изисквания на Закона за държавния служител (ЗДСл), Закон за защита на личните данни (ЗЗЛД), Кодекса на труда (КТ), Кодекса за социално осигуряване (КСО), Закона за счетоводството (ЗСч), Закона за противодействие на корупцията (ЗПК) и тн.

(3) Използването за служебни цели на събраните и съхранявани в регистър „Управление на човешките ресурси“ данни за съответните лица се отнася до:

1. дейности, касаещи съществуването, изменението и прекратяването на служебните и трудови правоотношения; изготвяне на всякакви документи на лицата в тази насока (заповеди, договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и тн.);

2. установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;

3. водене на счетоводна отчетност относно възнагражденията и разходите за командировки на работниците/служителите, за изплащане на заплати и обезщетения, за изпълнение на изискванията по ЗДСл и КТ.

(4) Данните в регистър „Управление на човешките ресурси“ се обработват на хартиен и електронен носител.

(5) В случаите, когато регистър „Управление на човешките ресурси“ се води на хартиен носител, се спазват следните правила:

1. лични данни, обработвани на хартиен носител се съхраняват в дирекция „Административно-правно обслужване и човешки ресурси“ (АПОЧР) в отделни досиета;

2. личните досиета се подреждат в специални картотечни шкафове със заключване, които са разположени в помещения на дирекция АПОЧР;

3. работниците/служителите в дирекция АПОЧР, отговарящи за човешките ресурси, са длъжностните лица, които, в качеството си на оператори на лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните досиета, в т.ч. ограничаване на достъпа до тях на други работници/служители и външни лица;

4. личните досиета на работниците/служителите на ДАБ при МС не се изнасят извън сградата на администратора;

(6) В случаите, когато регистър „Управление на човешките ресурси“ се води на технически носител, се спазват следните правила:

1. личните данни се въвеждат (в база данни и отделни файлове) на компютрите на обработващите лични данни, които са свързани в локална мрежа, със защитен достъп до личните данни;

2. достъп имат само обработващите лични данни, чрез предоставена парола;

3. компютрите са изолирани в помещения за самостоятелна работа;

4. защитата на електронните данни от неправомерен достъп се осигурява, чрез поддържане на антивирусни програми, периодично архивиране на данните, както и чрез поддържане на информацията и на хартиен носител.

(7) Обработваните, в регистър „Управление на човешките ресурси“, данни се предоставят от физическите лица при кандидатстване за работа по служебни и трудови правоотношения или при сключване на граждански договор с физическо лице и се въвеждат директно в заповедта за назначаване, в трудови или граждански договори, допълнителни

споразумения, както и в други документи, удостоверяващи трудов стаж, осигурителен стаж, служебни бележки, справки, удостоверения и кореспонденция.

(8) Данните относно здравословното състояние се представят в болнични листове от работника/служителя или заключения на Службата по трудова медицина, регистрират се в електронно приложение „Акстър", без да се сканират, след което се предават в дирекция „Финансово-счетоводни дейности".

Чл. 16 (1) В регистър „Кандидати за работа" се обработват лични данни за кандидати за работа в ДАБ при МС, както следва:

1. физическа идентичност-имена, ЕГН, адрес, телефон, електронна поща;

2. социална идентичност-образование, трудова дейност, квалификация;

3. медицинско свидетелство и свидетелство за съдимост при започване на работа;

4. семейно положение;

5. здравен статус;

6. данни за номера на банкова сметка с оглед изплащане на служебни и трудови възнаграждения и обезщетения.

(2) Обработката и съхранението на лични данни в регистър „Кандидати за работа" се извършва при и по повод изпълнение на нормативните изисквания на ЗДСл, ЗЗЛД, Кт, КСО, Наредбата за провеждане на конкурсите и подбора при мобилност на държавни служители.

(3) Използването за служебни цели на събраните и съхранявани в регистър „Кандидати за работа" данни за съответните лица е свързано с дейности по възникване на служебни и/или трудови правоотношения (за изготвяне на заповеди; договори; документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения).

(4) Данните в регистър „Кандидати за работа" се обработват на хартиен носител при спазване на следните правила:

1. личните данни се съхраняват в дирекция АПОЧР;

2. подреждат се в специални картотечни шкафове със заключване, разположени в дирекция АПОЧР;

3. работниците/служителите в дирекция АПОЧР, отговарящи за човешките ресурси са длъжностни лица, в качеството си на оператори на лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни, в т.ч. и ограничаване на достъпа до тях на други работници/служители и външни лица;

Чл. 17 (1) В регистър „Доставчици-изпълнители по договори" се обработват лични данни на физически лица, контрагенти на ДАБ при МС, както следва:

1. на изпълнители по граждански договори (отделни физически лица, вкл. и такива, представляващи юридически лица, търговски дружества)- имена, ЕГН, данни от лична карта и банкови сметки;

2. на изпълнители по договори за възлагане на обществени поръчки-лични данни на физически лица, представляващи юридически лица (търговски дружества, граждански дружества по Закона за задълженията и договорите), изискани и предоставяни в ДАБ при МС при и по повод възлагане на обществени поръчки по реда на Закона за обществените поръчки (ЗОП), Правилника за прилагане на Закона за обществените поръчки (ППЗОП).

(2) Личните данни в регистър „Доставчици-изпълнители по договори" се обработват във формата на хартиен носител при спазване на следните правила:

1. личните данни се съхраняват в дирекция ФСД в отделни досиета, в шкафове, снабдени със секретни заключващи устройства;

2. личните досиета се подреждат в специални картотечни шкафове със заключване, разположени в дирекция ФСД;

3. работниците/служителите в дирекция ФСД са длъжностни лица, в качеството си на оператори на лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(3) В случаите, когато регистър „Доставчици-изпълнители по договори" се води на електронен носител, се спазват следните правила:

1. личните данни се въвеждат (в база данни и отделни файлове) чрез компютрите на операторите на лични данни, свързани в локална мрежа, със защитен достъп до личните данни;

2. достъп имат само операторите на лични данни;

3. компютрите са изолирани в помещения за самостоятелна работа;

4. достъп до операционната система, съдържаща файлове за обработка на лични данни, имат само обработващите лични данни чрез парола.

(4) Оценката на въздействие се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 18 (1) В регистър „Възнаграждения и други плащания на персонала“ се обработват лични данни на работниците/служителите на ДАБ при МС, както следва: имена, ЕГН, данни от лична карта, банкова сметка.

(2) Личните данни в регистър „Възнаграждения и други плащания на персонала“ се обработват на хартиен носител при спазване на следните правила:

1. личните данни се класифицират и съхраняват в дирекция ФСД, в хронологично номерирани ведомости;

2. хронологично номерираните ведомости се съхраняват в шкафове, снабдени със заключващи устройства, разположени в помещения на дирекция ФСД;

3. работниците/служителите в дирекция ФСД са длъжностни лица, в качеството си на оператори на лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(3) В случаите, когато регистър „Възнаграждения и други плащания на персонала“ се води на електронен носител, се спазват следните правила:

1. личните данни се въвеждат (в база данни и отделни файлове) чрез компютрите на операторите на лични данни, свързани в локална мрежа, със защитен достъп до личните данни;

2. достъп имат само операторите на лични данни;

3. компютрите са изолирани в помещения за самостоятелна работа;

4. достъп до операционната система, съдържаща файлове за обработка на лични данни, имат само обработващите лични данни чрез парола.

(4) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване и/или унищожаване се осигурява чрез поддържане на антивирусни програми, периодично архивиране на данните, както и чрез поддържане на информацията на хартиен носител.

Чл. 19 (1) В регистър „Обществени поръчки“ се събират, обработват и съхраняват лични данни на физически лица, представляващи юридически лица (търговски дружества, граждански дружества по Закона за задълженията и договорите), изискани и предоставени в ДАБ при МС при и по повод възлагане на обществени поръчки по реда на ЗОП и ППЗОП.

(2) Личните данни се съхраняват в дирекция УСОП в отделни досиета, в шкафове, снабдени със секретни заключващи устройства.

Чл. 20 (1) В регистър „Чужденците с изготвен интеграционен профил“ се обработват лични данни на чужденци, търсещи международна закрила, както следва:

1. имена;

2. дата на раждане;

3. пол;

4. ЛНЧ;

5. семейно положение;

6. гражданство;

7. ниво на образование;

8. професионален опит/придобит стаж в държавата по произход;

9. професионална квалификация.

(2) Личните данни на чужденците- субекти на лични данни, се събират с тяхното съгласие.

(3) При водене на регистър „Чужденци с изготвен интеграционен профил“ се спазват следните правила:

1. личните данни се класират и съхраняват в дирекция „Социална дейност и адаптация“ (СДА) в отделни досиета;

2. досиетата се подреждат в шкафове, разположени в дирекция СДА;

3. работникът/служителят, отговарящ за регистър „Чужденци с изготвен интеграционен профил“ е длъжностно лице в дирекция СДА, което предприема всички организационно-технически мерки за съхраняването и опазването на досиетата;

4. интеграционните профили на чужденците не се изнасят извън сградата на администратора.

Чл. 21 (1) В регистър „Декларации по Закона за противодействие на корупцията“ (ЗПК) се събират и обработват лични данни на физически лица- работници/служители в ДАБ при МС, назначени по служебно и трудово правоотношение, имащи качеството на задължени лица по ЗПК.

(2) В регистъра на декларациите по ал. 1 се събират и обработват следните категории лични данни:

1. имена на служителя;

2. ЕГН;

3. длъжностно качество на служителя;

4. наименование на структурното звено;

5. данни за икономическата и социална идентичност на лицето-декларатор.

(3) Личните данни се обработват на хартиен и електронен носител.

(4) При водене на регистъра на декларациите по ал. 1 се спазват следните правила:

1. личните данни се класират и съхраняват в човешки ресурси- дирекция АПОЧР, в отделни досиета. Съгласно изискванията на закона декларациите се подават на хартиен и електронен носител (CD).

2. Досиетата се подреждат в метални шкафове, снабдени със заключващи устройства.

3. Работници/Служители в човешки ресурси- дирекция АПОЧР, в качеството си на оператори на лични данни в регистъра на декларациите по ал. 1, предприемат всички организационно-технически мерки за съхраняването на досиетата.

Чл. 22 (1) В регистър „Видеонаблюдение“ се събират, обработват и съхраняват видеозаписи, създадени чрез използване на технически средства за видеонаблюдение от подходите на сградите на ДАБ при МС и помещенията с определен статут, включително сградите на териториалните поделения. Записите с видеообрази се съхраняват на отделни персонални компютри монтирани в помещенията на физическата охрана на съответния обект.

(2) Личните данни, във формата на технически носител, се съхраняват и обработват на технически носители DVR, чрез автономна операционна система.

(3) Личните данни се предоставят доброволно от лицата при влизането им в сградата на ДАБ при МС или на територията на поделенията й. На входовете на сградите са поставени информационни табели, че обектите се намират под постоянно видеонаблюдение.

(4) Физическата защита на сградите се осъществява от денонощна физическа охрана.

IV. ОГРАНИЧЕНИЕ НА СЪХРАНЕНИЕТО

Чл. 23 (1) ДАБ при МС съхранява лични данни на хартиен и/или електронен носител, само за времето, необходимо за изпълнение на дейностите за обработката им и/или нормалното му функциониране, или когато в нормативен документ е определен друг период за тяхното съхранение.

(2) След изтичане срока на съхранение на личните данни, съгласно приложимата законова уредба, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(3) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожаването технически възможности (чрез разрязване с помощта на машина-шредер и/или чрез изгаряне) или ДАБ при МС възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Унищожаването се извършва след изрично издадена заповед на Председателя на ДАБ при МС и с утвърден от Държавен архив акт за унищожаване.

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

Чл. 24 (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 ДАБ при МС. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при:

1. първоначалното въвеждане на нови технологии;

2. автоматизирано обработване, включително профилиране или автоматизирано вземане на решения;

3. обработване на чувствителни лични данни в голям мащаб;

4. мащабно, систематично наблюдение на публично обществена зона;

5. други операции по обработване, съдържащи се в списък на надзорния орган по чл. 35, пар. 4 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

(3) Оценката на риска съдържа най-малко:

1. системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора на лични данни законен интерес;

2. оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

3. оценка на рисковете за правата и свободите на субектите на данни;

4. мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

(4) При извършването на оценката на въздействието се иска становището на длъжностното лице по защита на личните данни.

(5) В случай, че извършената оценка на въздействието покаже, че обработването ще породи висок риск, следва да се извърши консултация с Комисия за защита на личните данни преди планираното обработване.

Чл. 25 При внедряване на нов програмен продукт за обработване на лични данни следва да се състави комисия, която да направи мониторинг на възможностите на продукта с оглед спазване изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), както и на Закона за защита на личните данни и осигуряване на максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

VI. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 26 (1) ДАБ при МС предоставя лични данни в трети страни или на международни организации при спазване на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

(2) Данни от регистъра могат да бъдат предоставяни на държавни институции, с оглед изпълнение на нормативно задължение.

(3) Във връзка с използването на куриерски услуги-приемане, пренасяне и доставка и адресиране на пратките до съответния адресат ДАБ при МС посочва следните данни: имена, адрес, област, пощенски код и наименование на населеното място.

Чл. 27 (1) Работниците/служителите, заетите по граждански правоотношения, контрагентите, гражданите-заявители и жалбоподатели имат право на достъп до личните си данни, право на коригиране на личните им данни, право на изтриване, право на ограничаване на обработването, право на преносимост на данните и право на възражение.

(2) Лицата, за които се отнасят личните данни в регистрите, по тяхно искане, изразено писмено могат да упражнят правата си по ал. 1. Подаването на заявление по електронен път става чрез електронен подпис по реда на Закона за защита на личните данни (ЗЗЛД).

(3) Заявлението съдържа името на лицето, в т.ч. и други данни, които го идентифицират, описание на искането, предпочитаната форма за предоставяне на достъп до личните данни, подпис, дата и адрес за кореспонденция, както и пълномощно, в случай, че заявлението е подадено от упълномощено лице. Заявлението се регистрира в деловодството на администратора на лични данни.

(4) Срокът за разглеждане на заявлението е един месец, считано от деня на подаване на заявлението в деловодството на администратора на лични данни, който може да бъде удължен с още два месеца, когато е необходимо повече време за събиране на личните данни на лицето.

Чл. 28 Когато личното дело на чужденец се предоставя на представител, работникът/служителят изисква документ за самоличност и такъв, удостоверяващ представителна власт. При отказ на достъп до личното дело, чужденецът или неговият представител се уведомят писмено.

Чл. 29 Достъп до личните данни на лицата, съдържащи се на технически носител, има само администраторът на лични данни, а в негово отсъствие достъп до тях имат оправомощените от администратора на лични данни работници/служители.

Чл. 30 Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение.

VII.ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ

Физическа защита на личните данни

Чл. 31 Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Сградата на ДАБ при МС е с контролиран достъп на външни лица.

2. Личните данни се обработват в кабинетите на лицата, в чиито длъжностни характеристики е определено задължението за обработване на данни от определени регистри.

3. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в шкафове в кабинетите на упълномощените лица.

4. Помещенията, в които се обработват лични данни, са оборудвани със заключване на вратите. Сградата на ДАБ при МС е оборудвана с пожарогасителни средства.

5. Комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни, само в присъствието на упълномощени служители/работници на ДАБ при МС.

Персонална защита на личните данни

Чл. 32 Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни са запознават с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), Закона за защита на личните данни, настоящите Вътрешни правила, Инструкцията за реда на обработване на лични данни и за техническите и организационни мерки за защита на личните данни, Политиката на ДАБ при МС за защита на личните данни относно служителите, Общи Методически указания за прилагане на Регламент (ЕС) 2016/679 (Общ Регламент относно защитата на личните данни), в т.ч. и във връзка с обмена на данни между Държавната агенция за бежанците при Министерския съвет и териториалните му поделения

2. Лицата, обработващи лични данни, подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в служебното/трудовото досие на всеки един работник/служител.

3. Лицата, обработващи лични данни, се запознават с опасностите за личните данни, обработвани от администратора на лични данни.

Документална защита на личните данни

Чл. 33 Документалната защита на личните данни се осъществява при спазване на следните мерки:

1. Регистрите с лични данни, обработвани от ДАБ при МС, се поддържат на хартиен и/или електронен носител.

2. Обработването на личните данни се извършва в рамките на работното време на ДАБ при МС.

3. Достъп до регистрите с лични данни, обработвани от ДАБ при МС, имат само работници/служители, в чиито длъжностни характеристики е определено задължение за обработване на данните, при спазване на принципа „Необходимост да се знае“ или на които е поставена конкретна задача.

4. Личните данни се събират само за конкретни цели, в съответствие с нормативните изисквания към ДАБ при МС.

5. Личните данни на хартиен носител се съхраняват в определените за целта служебни помещения в сградата на ДАБ при МС.

6. Личните данни могат да бъдат размножавани и разпространявани от упълномощените работници/служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

7. След изтичане на срока за съхранение документите от регистрите същите се унищожават. Унищожението се извършва след изрично издадена заповед на Председателя на ДАБ при МС посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности /чрез разрязване с помощта на машина-шредер и/или чрез изгаряне или разрушаване /отваряне/ на корпуса на носителя на данни и др./ или ДАБ при МС възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

Защита на автоматизираните информационни системи и/или мрежи

Чл. 34 Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните и регистрите, поддържани от ДАБ при МС се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен работник/служител има личен профил /потребителско име и парола/, с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът на лични данни създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на личните данни е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа.

4. Организационните мерки за гарантиране нивото на сигурност:

а) охрана на сградата на ДАБ при МС.

б) работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

в) при ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

VIII. ПРОЦЕДУРА ПО ДОКЛАДВАНЕ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 35 (1) При регистриране на неправомерен достъп/нарушение на сигурността до информационните масиви за лични данни или друго нарушение на сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), работникът/служителят, констатирал нова нарушение/инцидент, незабавно докладва на длъжностното лица по защита на личните данни на ДАБ при МС, а той от своя страна на Председателя на ДАБ при МС.

(2) След уведомяването по ал. 1 Длъжностното лице по защита на личните данни докладва на Комисия за защита на личните данни в рамките да 72 часа от констатацията /постъпилия сигнал/ на нарушението/инцидента.

(3) Уведомлението до Комисията за защита на личните данни съдържа следната информация:

1. Описание на нарушението на сигурността, категориите и приблизителният брой на засегнатите субекти на лични данни и категориите и приблизителното количество на засегнатите записи на лични данни;
2. Името и координатите за връзка на Председателя на ДАБ при МС;
3. Описание на евентуалните последици от нарушението на сигурността;
4. Описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

(4) След уведомяването по ал. 2 Председателят на ДАБ при МС, във взаимодействие с длъжностното лице по защита на личните данни на ДАБ при МС и Комисията за защита на личните данни, предприема необходимите мерки за предотвратяване или намаляване на последиците от неправомерния достъп/нарушението на сигурността както и възможните мерки за възстановяване на данните.

(5) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Председателят на ДАБ при МС, възлага на длъжностното лице по защита на личните данни да уведоми незабавно засегнатите физически лица.

Чл. 36 (1) При възникване и установяване на инцидент с наличните ресурси на лични данни се вземат мерки за ограничаване въздействието върху регистрите, доколкото това е обективно възможно.

(2) За инцидентите, касаещи обработването на лични данни се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на работника/служителя, извършил доклада, последствията от инцидента и мерките, които са предприети за отстраняването им.

IX. ДРУГИ УСЛОВИЯ

Чл. 37 Адресът, на администратора на лични данни, на който се приемат молби и заявления, касаещи предоставянето на лични данни е гр. София ,бул. „Княгиня Мария Луиза“ № 114Б.

Чл. 38 Цялостният контрол върху дейностите по обработка и съхранение на лични данни в ДАБ при МС се осъществява от администратора на лични данни.

Чл. 39 При неизпълнение на задълженията им, вменени в Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ЗЗЛД и настоящите Вътрешни правила, на съответните работници/служители, обработващи и съхраняващи лични данни, се налагат дисциплинарни наказания по реда на ЗДСл, КТ.

X. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано /“субект на данни“/.

§2. „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.

§3. „Обработване на лични данни“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

§4. „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

§5. „Администратор“ означава компетентният орган, който сам или съвместно с други органи определя целите и средствата за обработването на лични данни

§6. „Оператор на лични данни“ означава работник/служител на ДАБ при МС, който обработва лични данни под ръководството на администратора.

§7. „Регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до който се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или георграфски принцип.

XI. ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

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

§2. Всички работници/служители на ДАБ при МС, чиито трудови/служебни задължения включват обработване на лични данни, са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват.

§3. За изпълнение на настоящите Вътрешни правила отговаря главният секретар на ДАБ при МС.

§4. За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), Закона за защита на личните данни, както и действащото приложимо законодателство, което регламентира обработката на лични данни.

§5. Настоящите Вътрешни правила се преглеждат и актуализират при всяка промяна в нормативната уредба, но най-малко веднъж годишно от длъжностното лице по защита на личните данни.