Консолидирана версия

ПРАВИЛА ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ В ПРОКУРАТУРАТА НА РЕПУБЛИКА БЪЛГАРИЯ

(Утвърдени със Заповед № РД-02-12 от 16.07.2020 г., изм. със Заповед № РД-02-28 от 17.12.2021 г., изм. със Заповед № РД-02-29 от 23.11.2023 г. на главния прокурор)

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите правила имат за цел да регламентират механизмите за защита на личните данни, обработвани в Прокуратурата на Република България (ПРБ). Като отчита естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, ПРБ прилага подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването на лични данни се извършва в съответствие с Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) и Закона за защита на личните данни (ЗЗЛД). При необходимост, тези мерки се преглеждат и актуализират.

(2) Когато ПРБ обработва лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от и предотвратяването на заплахи за обществения ред и сигурност, се прилагат разпоредбите на Глава осма от ЗЗЛД.

(3) Когато ПРБ обработва лични данни за цели, различни от тези по ал. 2, се прилагат ОРЗД и съответните разпоредби от ЗЗЛД, които въвеждат мерки за неговото прилагане.

Чл. 2. (1) При обработването на лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания личните данни:

1. се обработват законосъобразно и добросъвестно. Когато правото на Европейския съюз или Законът за защита на личните данни предвижда специфични условия за обработването на лични данни, прокуратурата уведомява получателя на данните за тези условия и за задължението му да ги спазва;

2. се събират за конкретни, изрично указани и законни цели и не се обработват по начин, който е несъвместим с тези цели;

3. са подходящи, относими и не надхвърлят необходимото във връзка с целите, за които данните се обработват;

4. са точни и при необходимост се поддържат в актуален вид; предприемат се всички необходими мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват. Когато предадените лични данни са неточни или са предадени незаконосъобразно, получателят се уведомява незабавно и се предприемат действия по коригиране, изтриване или ограничаване обработването на личните данни;

5. се съхраняват във вид, който позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимия за целите, за които те се обработват;

6. се обработват 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.

(2) Лични данни, първоначално събрани от ПРБ или друг администратор за други цели, могат да се обработват при необходимост и пропорционално на целите по ал. 1 в съответствие с правото на Европейския съюз или Закона за защита на личните данни.

(3) Когато е възможно, при обработването на лични данни за целите по ал. 1 се прави ясно разграничение между личните данни на различни категории субекти на данни-участници в наказателното производство.

(4) Обработването на лични данни е законосъобразно, когато е необходимо за упражняване на правомощията на ПРБ за целите по ал. 1 и е предвидено в правото на Европейския съюз или в нормативен акт, в който са определени целите на обработването и категориите лични данни, които се обработват.

Чл. 3. (1) За целите на дейността на администрацията Прокуратурата на Република България обработва личните данни в съответствие с принципите, установени в чл. 5 от ОРЗД, а именно:

а) законосъобразност, добросъвестност и прозрачност – обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

б) ограничение на целите на обработване – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

в) съотносимост с целите на обработката и свеждане до минимум на събираните данни – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;

г) точност и актуалност на данните – 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;

д) ограничение на съхранението с оглед постигане на целите – данните 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;

е) цялостност и поверителност на обработването и гарантиране на подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

ж) отчетност, който принцип дава възможност на администратора да докаже спазването и добросъвестното прилагане на посочените принципи.

(2) Лични данни се обработват само в случаите, когато е налице поне едно от посочените в чл. 6 на Регламент (ЕС) 2016/679 основания за обработване.

II. АДМИНИСТРАТОР И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 4. (1) *Администратор на лични данни* е Прокуратурата на Република България - юридическо лице на бюджетна издръжка със седалище София, Булстат: 121817309, адрес: гр. София, бул. „Витоша“ № 2.

(2) Структурните звена на ПРБ по чл. 136 от ЗСВ и учебните и почивни бази - третостепенни разпоредители с бюджет, са *структури с право на достъп до лични данни при администратора-ПРБ.*

(3) Административните ръководители на структурни звена в ПРБ, директорът на НСлС и ръководителите на учебни и почивни бази отговарят за прилагането на мерките за защита на личните данни в ръководените от тях структури по ал. 2.

Чл. 5. (1) Достъпът и обработването на лични данни се осъществява само от лица, чиито служебни задължения (по длъжностна характеристика) или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае“. Тези лица – магистрати и съдебни служители, действат *под ръководството и по указания* на администратора и са длъжни да познават и прилагат нормативната уредба в областта на защитата на личните данни, настоящите Правила, както и да отчитат рисковете за правата и свободите на физическите лица, чиито лични данни се обработват в ПРБ. *Лицата под ръководството* на администратора подписват декларация или се задължават с длъжностната характеристика да не разгласяват личните данни, до които са получили достъп при и по повод изпълнение на задълженията си.

(2) Запознаването с материали по преписки на ПРБ следва да се извършва при спазване на ограниченията, свързани със защитата на лични данни на трети лица.

Чл. 6. При неспазването на ограниченията за достъп до личните данни и нарушаване на правилата за обработване на лични данни магистратите и съдебните служители носят дисциплинарна отговорност.

Чл. 7. (1) Прокуратурата на Република България обработва личните данни самостоятелно или чрез възлагане на обработващи лични данни.

(2) *Обработващ лични данни* е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора на лични данни-ПРБ или от името на структурите с право на достъп до лични данни по чл. 4, ал. 2.

(3) ПРБ и структурите с право на достъп до лични данни по чл. 4, ал. 2 могат да възложат обработването на лични данни от свое име само на обработващи лични данни, които предоставят достатъчни гаранции, че ще прилагат подходящи технически и организационни мерки по такъв начин, че обработването да отговаря на изискванията на ОРЗД, съответно на глава осма от ЗЗЛД и да се гарантира защитата на правата на субекта на данни.

III. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл. 8. (1) Длъжностното лице по защита на данните се определя с акт на главния прокурор за защитата на личните данни, обработвани за цели, различни от тези по чл. 1, ал. 2.

(2) За длъжностно лице може да бъде определен прокурор от ВКП/ВАП, следовател от НСлС или съдебен служител от АГП.

(3) Данните за контакт с длъжностното лице се публикуват на интернет страницата на ПРБ - www.prb.bg и се съобщават на Комисията за защита на личните данни (КЗЛД) по образец на уведомление, утвърден от КЗЛД.

Чл. 9. Длъжностното лице по защита на данните се отчита пряко пред главния прокурор и има следните задължения и отговорности:

1. да предоставя съвети по отношение на оценката на въздействието върху защитата на лични данни;

2. да информира и консултира/съветва главния прокурор и ръководителите на структурите с право на достъп по чл. 4, ал. 2;

3. да наблюдава спазването на нормативните изисквания в областта на личните данни, включително повишаването на осведомеността и обучението на магистрати и съдебни служители, както и на служителите от звено "Вътрешен одит";

4. да допринася за повишаване на осведомеността на служителите в администрацията на ПРБ по въпроси, свързани със защитата на личните данни;

5. да спазва конфиденциалността на изпълняваните задачи;

6. да си сътрудничи с КЗЛД;

7. да действа като точка за контакт за КЗЛД.

8. да води регистъра на дейностите по обработване на личните данни.

Чл. 10. Длъжностното лице по защита на данните има право да изисква информация, справки и съдействие за изпълнение на задълженията си от всички структури по чл. 4, ал. 2.

IV. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 11. (1) Дейностите по обработване на лични данни, извършвани при осъществяване на правомощията на прокуратурата, се описват в регистър с категориите дейности по обработване на лични данни съгласно чл. 62 от ЗЗЛД. При поискване ПРБ предоставя достъп до регистъра на Инспектората към ВСС. Регистърът се поддържа в писмена форма, включително в електронен формат.

(2) В системите за автоматизирано обработване, поддържани от ПРБ, се водят системни дневници (логове) най-малко за следните операции по обработване – събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване. При извършване на справка или разкриване на данни тези дневници трябва да дават възможност за установяване на основанието, датата и часа на тези операции и доколкото е

възможно – идентификацията на лицето, което е направило справката или е разкрило личните данни, както и данни, идентифициращи получателите на тези лични данни.

(3) Дневниците се използват единствено за проверка на законосъобразността на обработването, за самоконтрол, за гарантиране на цялостността и сигурността на личните данни и при наказателни производства.

(4) Администраторът на лични данни определя подходящи срокове за съхранение, включително архивиране на дневниците по ал. 2. При поискване ПРБ предоставя дневниците по ал. 2 на надзорния орган.

Чл. 12. (1) Дейностите по обработване на лични данни, извършвани при осъществяване на дейността на администрацията на ПРБ, се описват в „Регистър на дейностите по обработване", съгласно чл. 30, параграф 1 от ОРЗД. ПРБ поддържа в писмена форма, включително в електронен формат, регистъра на дейностите по обработване, за които отговаря.

(2) Регистърът на дейностите по обработване на администратора се съставя от администратора ПРБ и се поддържа в актуален вид от Длъжностното лице по защита на данните и се предоставя на надзорния орган при проверка.

(3) Сроковете за съхранение на данните се посочват поотделно за всяка дейност по обработване в Регистъра на дейностите по обработване на лични данни в ПРБ, при съобразяване на Номенклатурата на делата в ПРБ.

Чл. 13. (1) Дейности по обработване на лични данни се извършват при осъществяване на правомощията на прокуратурата, както и при осъществяване на дейността на администрацията на ПРБ.

(2) **Дейности по обработване при изпълнение на правомощията на прокуратурата:**

1. Цели на обработване:

Обработването на лични данни е свързано с изпълнението на правомощията на прокуратурата, изпълнението на нормативно установените функции и задължения на прокурорите и следователите във връзка с дейностите по предотвратяване, разследване, разкриване, наказателно преследване и изпълнението на наказанията (ЗСВ, НПК, АПК, ЗИНЗС).

2. Категории субекти на данни:

Лица по прокурорски преписки, участници в досъдебното и съдебното производство, лица с наложени наказания.

3. Категории лични данни:

Данни, свързани с физическата идентичност – име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис, както и други данни, събирани и съхранявани в хода и за нуждите на разследването.

4. Категории получатели, пред които се разкриват личните данни:

Личните данни се разкриват на субектите на данни и лицата, предвидени в нормативен акт.

(3) **Дейности по обработване при осъществяване на дейността на администрацията на ПРБ:**

1. **Дейности по обработване при управлението на човешки ресурси**:

Цели на обработване:

Лични данни се обработват за индивидуализирането на правоотношенията с магистратите по ЗСВ, на трудовите и гражданските правоотношения, при спазване на нормативните изисквания - ЗСВ, ПАПРБ, КТ, ЗЗД, КСО, ЗСч, ЗДДФЛ, ЗНАФ, НРВПО и др.; за постигане на служебни цели; за внасянето на промени във вече възникнали правоотношения, за изготвянето на документи във връзка с правоотношенията /трудови договори, допълнителни споразумения, акт за заемане на длъжност, акт за изменение на акт за заемане на длъжност, граждански договори, документи, удостоверяващи различни видове стаж, служебни бележки, справки, удостоверения;за изготвяне на документи, свързани с повишаване ранга и/или размера на индивидуалния размер на основната месечна заплата, и др./, както и документи, необходими за представяне пред различни институции - по искане на служител, магистрат или държавни институции; за установяване на връзка със служители и магистрати по телефон; за изпращане на кореспонденция във връзка с изпълнение на задължения по сключените със служителите договори, издаване на служебни карти и др.

Категории субекти на данни:

При управлението на човешки ресурси се обработват лични данни на кандидати за работа на магистрати, съдебни служители и на изпълнители по граждански договори.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис; с икономическата идентичност - имотно състояние, имущество и интереси; със социалната идентичност - образование, трудова дейност; данни за здравословното и психическото състояние (медицинско свидетелство, удостоверение за психическо състояние, болнични листове и др.); данни за съдимост (свидетелство за съдимост); лични данни, свързани с гражданството (декларация), с наличието или липсата на качеството на обвиняем по неприключени наказателни производства (удостоверения);данни, свързани с деклариране на липса на несъвместимост (декларация); данни, свързани със семейно положение, родствени връзки, както и данни, свързани с политически неутралитет (декларация).

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни (Служба по трудова медицина), субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, съдилища, съдебни изпълнители, ВСС, Инспектората към ВСС, НИП и др.

2. Дейности по обработване при осъществяването на финансово-стопанската дейност:

Цели на обработване:

Лични данни се обработват за изпълнение на задълженията, свързани с воденето на счетоводна отчетност, изплащането на възнагражденията на служители и магистрати, на третите лица-изпълнители по договори за доставка на стоки и услуги, за погасяването на задължения по предявени за плащане изпълнителни листове, изплащане на възнаграждения на вещи лица, преводачи и др.

Категории субекти на данни:

Прокурори, следователи, съдебни служители и изпълнители по граждански договори, трети лица - контрагенти, кредитори, длъжници, както и участници в наказателното производство - вещи лица, преводачи и др.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон.

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, ЧСИ, ВСС, АДФИ, Сметната палата и др.

3. Дейности по обработване по направление правни дейности:

Цели на обработване:

Лични данни се обработват за служебни цели - изготвяне на становища, докладни записки, проекти на документи - решения, писма, съдебни книжа, заповеди, молби и др., при съобразяване с нормативните изисквания по ЗДОИ, ЗЗЛД, ГПК, АПК, КСО, ЗСВ, КТ и др., за установяване на връзка със субекта на данни – за изпращане на кореспонденция, за провеждане на процедури по възлагане на обществени поръчки по ЗОП, сключване на договори за доставки и др.

Категории субекти на данни:

Обработват се лични данни на молители, жалбоподатели, заявители, кандидати и участници в процедури за възлагане на обществени поръчки, изпълнители на обществени поръчки, служители.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон, подпис, лични данни за образование, професионална квалификация.

Категориите получатели, пред които се разкриват личните данни:

Агенция за обществени поръчки, съдебни органи, съдебни изпълнители, участници в процедурите за възлагане на обществени поръчки, обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт и др.

4. Дейности по обработване, свързани с осъществяването на контролиран достъп до определени места в съдебните сгради или охраната на стопанисвани имоти:

Цели на обработване:

Обработването на лични данни се извършва за целите на осъществяване на контролиран достъп до сгради, помещения и стопанисвани имоти.

Категории субекти на данни:

Всички магистрати и служители на ПРБ, външни лица/посетители, гости, изпълнители по договори, почиващи.

Категории лични данни:

Обработват се образи на лицата, съдържащи се в снимки и видеозаписи.

Категориите получатели, пред които се разкриват личните данни:

Органи на разследване, наблюдавани лица.

5. Дейности по обработване на лични данни, свързани с осъществяването на обучителни мероприятия и почивка:

Цели на обработване:

Обработването на лични данни се извършва за осигуряване на почивка на магистрати и съдебни служители на ПРБ и членовете на техните семейства и други придружаващи лица, извън членовете на семействата, както и за целите на провежданите обучителни мероприятия.

Категории субекти на данни:

Прокурори, следователи, съдебни служители и членове на техните семейства, преподаватели/обучители, гости.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон, и със семейната идентичност – родствени връзки.

Категориите получатели, пред които се разкриват личните данни:

Общинска администрация.

6. Дейности по обработване на лични данни, свързани с издаване на удостоверителни документи/удостоверения за наличие или липса на повдигнати обвинения по неприключени наказателни производства спрямо конкретно лице.

Цели на обработване:

Обработването на лични данни се извършва за изготвяне на удостоверителни документи в изпълнение на законови изисквания.

Категории субекти на данни:

Обработват се лични данни на физически лица.

Категории лични данни, свързани с физическата идентичност – име, ЕГН, адрес, данни на лична карта, телефон.

Категории получатели, пред които се разкриват лични данни:

Служби за сигурност и служби за обществен ред по смисъла на Закона за защита на класифицираната информация, държавни институции, физически и юридически лица.

(4) Личните данни се обработват на хартиен и технически носител и се съхраняват в срокове, съгласно действащата в ПРБ номенклатура на делата.

Чл. 13а. Отбелязване на срока за съхранение в Регистъра на дейностите по обработване на лични данни:

1. винаги, когато това е възможно, длъжностното лице по защита на данните записва предвидените срокове за изтриване на различните категории данни в Регистъра на дейностите по обработване, съгласно чл. 30, пар. 1, б. „е“ от Регламент (ЕС) 2016/679, респ. чл. 62, ал. 1, т. 8 от ЗЗЛД.

2. при наличие на промени в сроковете за изтриване, произтичащи от нормативен акт или от Номенклатурата на делата на ПРБ, регистърът на дейностите на администратора-ПРБ се актуализира от длъжностното лице по защита на данните.

V. ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

1. ОСИГУРЯВАНЕ НА ПРОЗРАЧНОСТ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 14. (1) При събиране на лични данни от ПРБ за целите на дейността на администрацията, чрез структурите с право на достъп по чл. 4, ал. 2 на субектите на лични данни се предоставя следната информация в момента на получаването на личните данни:

1. данните, които идентифицират администратора и координатите за връзка с него;

2. координатите за връзка с длъжностното лице по защита на данните;

3. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването им;

4. получателите или категориите получатели на личните данни;

5. срокът, за който ще се съхраняват личните данни;

6. правото на субекта на данни да изиска достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни или правото да се прави възражение срещу обработването, както и правото на преносимост на данните;

7. правото на субекта на данни да подаде жалба до КЗЛД или до съда;

8. дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключване на договор, както и дали субектът на данните е длъжен да предостави личните си данни или да декларира съгласие за обработването им, и евентуалните последствия, ако тези данни или декларацията не бъдат предоставени.

(2) Информация се предоставя в обобщена, кратка и разбираема форма на интернет сайта на ПРБ и на структурите по чл. 4, ал. 2, както и/или по друг подходящ начин.

Чл. 15. (1) За обработваните лични данни за целите по чл. 1, ал. 2 на субекта на лични данни се предоставя най-малко следната информация:

1. данните, които идентифицират администратора, и координатите за връзка с него;

2. целите, за които се обработват личните данни;

3. правото на жалба до Инспектората на ВСС (Инспекторат) и координатите му за връзка;

4. правото да се изиска от администратора достъп до коригиране, допълване или изтриване на лични данни и ограничаване на обработването на лични данни, свързано със субекта на данните;

5. възможността за упражняване на правата му чрез Инспектората при отказ или ограничаване на достъпа по чл. 54, ал. 3, по чл. 55, ал. 3 и ал. 4 и чл. 56, ал. 6 и ал.7 от ЗЗЛД.

(2) По искане на субекта на данни или по своя инициатива, администраторът предоставя на субекта на данни следната допълнителна информация:

1. правното основание за обработването;

2. срокът, за който ще се съхраняват личните данни, а ако това е невъзможно – критериите за определянето на този срок;

3. когато е приложимо, получателите или категориите получатели на лични данни, включително в трети държави или международни организации;

4. когато е необходимо, и друга допълнителна информация, по-специално в случаите, когато личните данни са събрани без знанието на субекта на данните.

(3) Предоставянето на информацията по ал. 2 се забавя или отказва изцяло или частично, когато това е необходимо, за да не се допусне възпрепятстване на проверки, разследвания или процедури или неблагоприятно засягане осъществяването на целите по чл. 1, ал. 2, за да се защитят обществения ред и сигурност, националната сигурност и правата и свободите на други лица.

Чл. 16. Ръководителите по чл. 4, ал. 3 определят подходящи процедури, които да определят начините и средствата за изпълнение на задълженията по осигуряване на прозрачност при обработването на лични данни в ПРБ.

2. ДЕЙСТВИЯ ПРИ НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 17. (1) В случай на нарушение на сигурността на личните данни, ръководителите на структурите по чл. 4, ал. 2 са длъжни незабавно след узнаването да уведомят главния прокурор, който е длъжен да уведоми КЗЛД, съответно Инспектората към ВСС, за нарушението на сигурността на личните данни, не по-късно от 72 часа след узнаването, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица.

(2) Под нарушение на сигурността на личните данни се имат предвид всички събития, които водят до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

Чл. 18. (1) Администраторът документира в „Регистър на нарушенията на сигурността“ всички нарушения на сигурността на личните данни, като посочва отнасящите се до тях факти, последиците и предприетите мерки за смекчаване на тяхното въздействие.

(2) „Регистърът на нарушенията на сигурността“ се поддържа от длъжностното лице по защита на личните данни.

Чл. 19. (1) Когато нарушението на сигурността на личните данни е вероятно да породи висок риск за правата и свободите на физическите лица, ръководителите по чл. 4, ал. 3, без ненужно забавяне, съобщават на субекта на данните за нарушението на сигурността на личните данни, освен когато:

1. са предприети подходящи мерки за защита и тези мерки са приложени по отношение на личните данни, засегнати от нарушението;

2. са взети впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

3. това би довело до непропорционални усилия.

(2) В случаите по чл. 15, ал. 3 администраторът може да не уведоми субекта на данните за нарушението по ал. 1, да го уведоми след 7-дневния срок, както и да ограничи информацията относно нарушението на сигурността.

3. ДРУГИ ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА

Чл. 20. Администраторът на лични данни - ПРБ осигурява необходимите финансови, технически и човешки ресурси за определянето и въвеждането на подходящи организационни и технически мерки, съответстващи на рисковете с различна вероятност и тежест за правата и свободите на физическите лица. За определянето на подходящи мерки във ВКП, ВАП, НСлС и АГП се назначава комисия, в чийто състав задължително участват директорите на дирекции ИОТ, БСД и АП в АГП.

Чл. 21. Административните ръководители на структурни звена в ПРБ и ръководителите на учебни и почивни бази определят служители в ръководените от тях структури по чл. 4, ал. 2 със следните отговорности:

- извършване на предварителен и последващ контрол на материалите, публикувани в интернет, за съответствие с нормативната уредба в областта на защитата на личните данни;

- извършване на преглед и предприемане на действия за актуализиране на договореностите с обработващите лични данни, декларациите и другите форми на документиране на съгласието на субекта на данни, както и на декларациите и длъжностните характеристики на служителите;

- извършване на периодични проверки за необходимостта от съхраняване на обработваните лични данни;

- изпитване за преценяване на ефективността на прилаганите технически и организационни мерки с оглед гарантиране на сигурността на обработваните лични данни, поне два пъти годишно;

- организиране и провеждане на първоначално обучение на новоназначени служители.

Чл. 22. Ръководителите на структурите с право на достъп по чл. 4, ал. 2 в ПРБопределят подходящи процедури, които дават възможност на служителите им пряко и поверително да им докладват за нарушения при обработването на лични данни за целите по чл. 1, ал. 2.

Чл. 22а. (1) Управляващите и контролиращите използването на информационните активи служители на ръководни длъжности в администрацията на ПРБ, със съдействието на длъжностното лице по защита на данните, когато е приложимо, следят за спазване на изискванията относно обработването на лични данни:

1. директорът на Дирекция „Информационно обслужване и технологии“ в АГП и съответните ръководители на административни звена или самостоятелни длъжности в направление „Информационно обслужване“ в общата администрация на прокуратурите следят за прилагане на правилата за мрежова и информационна сигурност по отношение на всички информационни активи, които са на електронен носител;

2. директорът на Дирекция „Бюджет и счетоводни дейности“ в АГП, съответните ръководители на административни звена или самостоятелни длъжности в направление „Финансово-стопанска дейност“ в апелативните, военно-апелативната, окръжните, военно-окръжните, Софийската градска и Софийската районна прокуратура, както и от направление „Финансово-счетоводна дейност“ на районните прокуратури, следят за спазване правилата за съхраняването на финансовите (счетоводни, осигурителни, данъчни) и свързаните с тях записи и документи;

3. ръководителят на отдел „Човешки ресурси“ в АГП и съответните ръководители на административни звена или самостоятелни длъжности в направление „Човешки ресурси“ в общата администрация на прокуратурите отговарят за спазване на правилата за съхраняването на всички записи, свързани с работата на съответните звена - назначаване, освобождаване, поддържане на кадрови досиета и други;

4. ръководителят на отдел „Правен“ в АГП следи за спазване правилата за съхраняване по отношение на разпределените на отдела документи и преписки;

5. ръководителят на Служба „Регистратура и деловодство“ в АГП и съдебните администратори и административните секретари в апелативните, военно-апелативната, окръжните, военно-окръжните, Софийската градска и районните прокуратури; на служби „Регистратура и деловодство“ и „Документално обслужване“ в Националната следствена служба, както и на служби „Регистратура“ и „Деловодство в отдел“ за администрацията във върховните прокуратури следят за спазване на правилата относно съхраняването, разпространяването и унищожаването на лични данни при извършване на документооборота в ПРБ;

6. съответните ръководители на служби „Архив“ следят за спазване правилата за съхраняването на документите в архивния фонд в ПРБ;

7. длъжностното лице по защита на данните следи за информираността на отговорните лица по въпросите на съхраняването на лични данни и своевременно предприема необходимите мерки при проблеми с тяхното прилагане;

8. всички останали служители в ПРБ спазват правилата относно съхраняването на лични данни, обработвани по повод осъществяване на тяхната дейност в ПРБ.

(2) Административните ръководители на структурни звена в ПРБ, директорът на НСлС и ръководителите на учебни и почивни бази, като отговорни лица за прилагането на мерките за защита на личните данни в ръководените от тях структури, отговарят и за спазването на правилата относно съхраняването на лични данни при обработване на лични данни по повод осъществяване на дейността на съответните структури.

(3) Директорът на Дирекция „Информационно обслужване и технологии" в АГП и съответните ръководители на административни звена или самостоятелни длъжности в направление „Информационно обслужване" в общата администрация на прокуратурите подпомагат лицата по ал. 1 и ал. 2 при осъществяване на задълженията им относно спазване на правилата за съхраняване на информационните активи.

VI. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ И ПРЕДВАРИТЕЛНИ КОНСУЛТАЦИИ

Чл. 23. Оценката на въздействието е процес, чиято цел е да опише обработването на личните данни, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, като ги оцени и определи мерки за справяне с тези рискове.

Чл. 24. (1) Ръководителите на структурите с право на достъп по чл. 4, ал. 2 могат да дават предложения за извършване на оценка на въздействието. Оценка на въздействието се извършва:

1. когато има вероятност операциите по обработването да доведат до висок риск за правата и свободите на физическите лица;

2. при операции на обработване съгласно оповестения от КЗЛД нарочен списък.

(2) При извършване на оценка на въздействието върху защитата на данните задължително се иска становището на длъжностното лице по защита на личните данни и дирекция ИОТ в АГП.

Чл. 25. Оценката съдържа най-малко:

1. системен опис на операциите по обработване и целите на обработване. Отчита се характера на обработваните лични данни – систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране); данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном; лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони; лични данни в широкомащабни регистри на лични данни; данни, чието обработване съгласно решение на КЗЛД застрашава правата и законните интереси на физическите лица;

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.

Чл. 26. (1) Оценката на въздействието се извършва при възникнала необходимост. Когато има промяна в риска, с който са свързани операциите по обработване, се прави преглед дали обработването е в съответствие с оценката на въздействието.

(2) Администраторът се консултира с надзорния орган всеки път, когато след извършена оценка на въздействието върху защитата на данните установи, че не може да предприеме достатъчни мерки за намаляване на рисковете до приемливо равнище.

Чл. 27. (1) При планирането на всяка дейност, която предвижда обработването на лични данни, администраторът извършва оценка на риска и ако е необходимо, оценка на въздействието върху защитата на данните (ОВЗД), като взема предвид вида на личните данни и начините за обработването им.

(2) Ръководителите на структурите с право на достъп по чл. 4, ал. 2, ръководещи отделните работни процеси по обработване на лични данни, са отговорни за своевременното известяване на длъжностното лице по защита на личните данни за наличието на нови дейности по обработване.

(3) Администраторът, с помощта на ДЛЗД, извършва оценка на риска и ОВЗД с цел определяне на адекватно ниво на технически и организационни мерки за защита на личните данни, което отговаря на обработваните от него лични данни и въздействието при нарушаване на защитата им.

(4) Администраторът оценява риска, като отчита вероятността за настъпване на съответното нарушение на сигурността на данните и величината на потенциалните неблагоприятни последици за субектите на данни.

(5) Оценка на въздействието върху защитата на данните се извършва задължително от администратора в следните случаи:

- при идентифициране на висок риск;
- в случай на извършване на систематична и подробна оценка на личните аспекти по отношение на физически лица при автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;
- при мащабно обработване на „чувствителни“ лични данни или на лични данни за присъди и нарушения;
- при систематично мащабно наблюдение на публично достъпна зона.

(6) Оценка на въздействието върху защитата на данните се извършва задължително и съгласно списък на видовете операции по обработване на лични данни, приет от КЗЛД, а именно:

- мащабно обработване на биометрични данни за целите на уникалната идентификация на физическо лице, което не е спорадично;
- обработване на генетични данни с цел профилиране, което поражда правни последици за субекта на данни или по подобен начин го засяга в значителна степен;

- обработване на данни за местоположение с цел профилиране, което поражда правни последици за субекта на данни или по подобен начин го засяга в значителна степен;

- при невъзможност за предоставяне на информация на субекта на данни по чл. 14 от Регламент (ЕС) 2016/679 или ако предоставянето на тази информация изисква несъразмерно големи усилия, или има вероятност да направи невъзможно, или сериозно да затрудни постигането на целите на обработване, когато това е свързано с мащабно обработване на данни;

- обработване на лични данни, осъществявано от администратор с основно място на установяване извън ЕС, когато определеният за негов представител в ЕС е разположен на територията на Република България;

- редовно и систематично обработване, при което предоставянето на информацията по чл. 19 от Регламент (ЕС) 2016/679 от администратора на субекта на данни е невъзможно или изисква несъразмерно големи усилия;

- обработване на лични данни на деца при пряко предлагане на услуги на информационното общество;

- осъществяване на миграция на данни от съществуващи към нови технологии, когато това е свързано с мащабно обработване на данни.

(7) Оценката на риска и оценката на въздействието се извършват на основата на избрана от администратора и съгласувана с ДЛЗД методология.

VII. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Гарантиране на цялостност, поверителност, наличност и достъпност на данните в срока за съхранение

Чл. 27а. (1) При извършване на всяка дейност по обработване на лични данни се спазват изискванията, произтичащи от приложимите нормативни актове за съответното обработване, както и основните технически и организационни мерки, предприети в ПРБ.

(2) Основните технически и организационни мерки обхващат мерките по отношение на магистрати и служители, физическа и документална защита, както и защитата на комуникационните и информационните системи и криптографската защита.

Чл. 28. (1) ПРБ като администратор на лични данни осигурява чрез ръководителите на структурите с право на достъп по чл. 4, ал. 2 подходящи технически и организационни мерки за осигуряване на ниво на сигурност, съобразено с рисковете за правата и свободите на физическите лица, през целия период на съхранение на личните данни. Техническите и организационните мерки трябва да гарантират цялостност, наличност, достъпност и поверителност.

(2) В структурите по чл. 4, ал. 2 се поддържа актуален списък на обработваните категории лични данни и въведените технически и организационни мерки за защита.

Чл. 29. При оценката на подходящото ниво на сигурност се вземат предвид преди всичко рисковете, свързани с обработването като случайно или неправомерно

унищожаване, загуба, промяна, неразрешено разкриване или достъп до обработвани лични данни.

Чл. 30. (1) Мерките могат да включват и псевдонимизация и криптиране на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите за обработване, способност за своевременно възстановяване на наличността и достъпа до лични данни в случай на физически или технически инцидент, процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационни мерки.

(2) Подходящите технически и организационни мерки се въвеждат към момента на определяне на средствата за обработване и към момента на самото обработване. Задължението за въвеждане на подходящи мерки се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.

(3) С мерките по ал. 2 администраторът на лични данни гарантира, че по подразбиране се обработват лични данни, които са необходими за всяка конкретна цел на обработването.

Чл. 31. Когато след извършена оценка на въздействието не е указано друго, в ПРБ се прилагат следните минимални технически и организационни мерки за защита на личните данни:

а) Физическа защита, която гарантира, че:

- помещенията, в които се съхраняват информационни активи с лични данни, се заключват;

- самостоятелен достъп до помещенията имат само оторизирани за това лица;

- хартиените информационни активи се съхраняват (по възможност) в заключени шкафове или каси, като самостоятелен достъп до тях имат само оторизираните за това лица;

- помещенията са оборудвани с пожароизвестителна система и пожарогасителни средства.

1. *Основни организационни мерки на физическа защита са*:

1.1. определяне на зони с контролиран достъп - в зоната с контролиран достъп се допускат лица, след проверка на документ за самоличност или служебна карта;

1.2. определяне на организацията на физическия достъп - достъп до помещенията, в които се обработват лични данни, имат определените за целта лица. Външни лица се допускат след прилагане на допълнителни мерки за защита на личните данни;

1.3. определяне на технически средства за физическа защита и определяне на екип за реагиране при нарушения.

2. *Основни технически мерки на физическа защита са*: ключалки, шкафове, метални каси, устройства за контрол на физическия достъп, охрана и/или система за сигурност, пожарогасителни средства, пожароизвестителни и пожарогасителни средства, детектори за субстанции.

б) Персонална защита, която гарантира, че:

- служителите са запознати със задълженията им като потребители на комуникационни и информационни системи (КИС), посочени във Вътрешните правила за мрежова и информационна сигурност на комуникационните и информационните системи на ПРБ;

- служителите са запознати и спазват принципа „Необходимост да знае“ - достъпът и обработването на лични данни се осъществява само от лица, чиито служебни задължения (по длъжностна характеристика) или конкретно възложена задача налагат такъв достъп;

- служителите са запознати, че при неспазването на ограниченията за достъп до личните данни и нарушаване на правилата за обработване на лични данни носят дисциплинарна отговорност;

- служителите са запознати със забраната за споделяне на критична информация между тях (като идентификатори, пароли за достъп и т.н.);

- служителите са запознати със забраната да се споделя неправомерно информация относно личните данни с трети страни извън организацията на администратора;

- служителите са запознати с реда за унищожаване на чернови и копия на документи;

- служителите са запознати с правилата за документооборот съгласно Инструкция за деловодната дейност и документооборота в Прокуратурата на Република България.

1. Лицата, обработващи лични данни под ръководството на администратора, при постъпване на работа се запознават с:

- нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане;
- опасностите за личните данни, обработвани от администратора;
- настоящите правила;
- мерките в конкретната структура по чл. 4, ал. 2, предприети за спазване на настоящите правила и всички други правила, процедури и указания на администратора, които се публикуват на ведомствения информационен сайт на ПРБ.

Тези документи се включват в програмата за обучение, което се провежда най-малко веднъж годишно. Веднъж годишно се провежда и тренировка на служители и магистрати за реакция при събития, застрашаващи сигурността на данните.

2. Служителите, обработващи лични данни, задължително трябва да притежават необходимата компютърна грамотност и умение за работа с използваните специализирани софтуерни продукти.

3. Лицата, обработващи лични данни под ръководството на администратора, задължително 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 кадровото досие на всеки служител. Подписването на декларация не се изисква, ако съответното задължение е включено в длъжностната характеристика на лицето.

в) Документална защита, която гарантира, че документите, съхранявани на хартиен носител, се обработват и съхраняват съобразно Инструкцията за деловодната дейност и документооборота в Прокуратурата на Република България:

1. Документите, съдържащи лични данни, се съхраняват само в помещения с ограничен достъп;

2. Обработването на лични данни на хартиен носител се извършва само в работно време, по изключение в извънработно време след разпореждане на административния ръководител;

3. Достъп до регистрите имат служителите в съответствие с принципа „Необходимост да знае";

4. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред;

г) Защита на комуникационните и информационни системи, която гарантира, че:

1. се спазват всички разпоредби на Вътрешните правила за информационна сигурност на автоматизираните информационни системи или мрежи в ПРБ. Електронната обработка на лични данни се реализира с помощта на специализирани приложни софтуерни продукти и чрез стандартни средства за текстообработка, електронни таблици и др. Използват само лицензирани системни и приложни софтуерни продукти или компютърни програми и бази данни, създадени по реда на Закона за авторското право и сродните му права. С цел възстановяване на данните от регистрите се подържат резервни копия за възстановяване на базите данни и на данните във файловата система;

2. комуникационните и информационни системи се конфигурират най-малкото до стандартно ниво на сигурност. В случай на установяване на висок риск за правата и свободите на субектите на данни при извършване на оценка на риска или оценка на въздействието върху защитата на данните, ДЛЗД чрез административните ръководители в ПРБ може да поиска увеличаване на нивото на сигурност;

3. връзката при комуникацията между клиента и сървъра при комуникацията по електронна поща се криптира - TLS (transport layer security) протокол;

4. достъпът на всеки потребител до информационните и комуникационните системи се осъществява с персонална парола, която отговаря на изискванията на Вътрешните правила за информационна сигурност на автоматизираните информационни системи или мрежи в ПРБ. Всеки упълномощен потребител на АИС/М има личен профил с определени нива на достъп, съобразни с неговите задължения и принципа „Необходимост да знае";

5. когато хардуерен информационен актив подлежи на предаване на трета страна, външен доставчик, информационният носител се отстранява предварително, така че да е невъзможен външен достъп до информацията;

6. при изваждане на компютър от активите (бракуване), информацията се изтрива по невъзвратим начин, като се използва специален софтуер – ОВАИ или друг аналогичен. Изтриването на лични данни обхваща и личните данни от резервните копия;

7. отношенията с всички трети страни, външни доставчици се определят по правилата на „Процедура за управление на процесите при работа с контрагенти".

д) Криптографска защита:

За криптографска защита се използват стандартните криптографски възможности на операционната система, на системите за управление на бази данни, на комуникационното оборудване, както и квалифицирани електронни подписи (КЕП).

Конкретни мерки по отношение на информационните активи

Чл. 31а (1) За всички информационни активи по съответната дейност се прилагат и следните конкретни мерки:

1. обработване на лични данни на кандидати за работа:

а) съхраняват се в помещенията и организационната структура на звеното по направление управление на човешки ресурси;

б) съхранението на оригинали или нотариално заверени копия на документи, които удостоверяват необходимата квалификационна степен и стаж за заеманата длъжност, се връщат на субекта на данни, който не е одобрен за назначаване, в 6-месечен срок от окончателното приключване на процедурата; вътрешни документи от проведения конкурс се съхраняват до 3 години.

2. обработване на лични данни на лица по трудови и служебни правоотношения и по граждански договори:

а) съхраняват се в помещенията и организационната структура по направление управление на човешки ресурси;

б) по отношение на използваната специализирана интегрирана компютърна система за работна заплата и управление на човешки ресурси се спазват правилата за ограничен достъп само от упълномощени потребители. Всеки потребител има своя персонална парола, която отговаря на изискванията на правилата за мрежова и информационна сигурност;

в) съхраняват се за срок 50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят: трудови договори, допълнителни споразумения, заповеди за назначаване, допълнителни споразумения/заповеди за преназначаване, заповеди за ползван неплатен отпуск общо над 30 работни дни в една календарна година, заповеди за прекратяване на трудови или служебни правоотношения (чл. 5, ал. 7 от КСО); останалите документи се съхраняват според сроковете, посочени в Номенклатурата на делата на ПРБ;

3. обработване на лични данни на служителите, които се събират във връзка с декларациите по Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество:

а) съхраняват се от звеното по направление Човешки ресурси. Декларациите имат входящ номер, съхраняват се в пликове и класьори в заключващи се каси;

б) декларациите в частта, която трябва да бъде публикувана на сайта на ПРБ, се публикува след обезличаване на ЕГН, подпис и само в частта относно интересите.

в) съхраняват се според сроковете, посочени в Номенклатурата на делата на ПРБ – 5 години след прекратяване на трудовото/служебното правоотношение, заедно с досието.

4. обработване при осъществяване на финансово-стопанската и финансово-счетоводната дейност - данни, които се обработват в организацията с цел изплащане на възнаграждения, обезщетения, погасяването на задължения по предявени за плащане изпълнителни листа и др.:

а) съхраняването на документите през текущата година се осъществява от звената по направление финансово-стопански дейности;

б) по отношение на използваната специализирана интегрирана компютърна система за счетоводство се спазват правилата за ограничен достъп само от упълномощени потребители. Всеки потребител има своя персонална парола, която отговаря на изискванията на Вътрешните правила за мрежова и информационна сигурност;

в) ведомости за заплати се съхраняват за срок от 50 г., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят (чл. 5, ал. 7 от КСО), останалите документи според сроковете, посочени в Номенклатурата на делата на ПРБ.

5. обработване на лични данни във връзка с командировки на магистрати и служители:

а) съхраняват се в помещенията на структурните звена по направление на дейност „Институционални и международни отношения“ на общата администрация в АГП и звената по направленията човешки ресурси и финансово-стопански дейности на общата администрация на прокуратурите;

б) съхраняват се в сроковете, посочени в Номенклатурата на делата на ПРБ;

6. обработване на лични данни във връзка с настаняване във ведомствени жилища на прокуратурата:

а) съхраняват се в отдел „Управление на собствеността“ в АГП;

б) съхраняват се в картотека, която се намира в заключени шкафове;

в) съхраняват се в срокове, посочени в Номенклатурата на делата на ПРБ, а данните за здравето - за срока на наемния договор;

7. обработване на лични данни на магистрати и служители, които ползват служебни телефони и сим-карти:

а) съхраняват се в звената по направленията човешки ресурси и финансово-стопански дейности;

б) съхраняват се в срокове, посочени в Номенклатурата на делата на ПРБ;

8. обработване на лични данни по направление правни дейности:

а) лични данни, обработвани във връзка с провеждане на обществени поръчки, се съхраняват в звената по направление обществени поръчки/финансово-стопански дейности. Поддържа се вътрешен електронен регистър *(в който се вписват данни, например, за номер на договора, предмет, изпълнител, срок, основание и др.)*, достъпът до който се осъществява

само от оторизирани лица, разполагащи с персонална парола за компютърната система, в която той се поддържа. Сроковете за съхранение са посочени в Номенклатурата на делата на ПРБ;

б) лични данни във връзка с подаване на сигнали по дейността се приемат от Служба „Регистратура и деловодство“ и могат да се обработват от други организационни единици в зависимост от сигнала. Съхраняват се в срокове, посочени в Номенклатурата на делата на ПРБ;

в) обработване на лични данни на лица, искащи достъп до обществена информация – съхраняват се в звеното по правни дейности в АГП и в службите „Регистратура, деловодство и архив“ в прокуратурите за срок от 1 (една) година в случай на уважено искане за достъп или необжалван отказ, а в случай на обжалване - 1 година след приключване на делото.

9. обработване на лични данни, свързани с дейността на учебните и почивните бази на ПРБ:

а) съхраняват се в Дирекция „СФОП“ /за АГП/ и се обработват със специализиран софтуер за регистрация на посетителите на място в почивните бази.

б) достъпът до данните, обработвани в почивните бази, се осъществява само от оторизирани служители с права на достъп. Всеки потребител има своя персонална парола, която отговаря на изискванията за мрежова и информационна сигурност в ПРБ.

в) съхраняват се за сроковете, посочени в Номенклатурата на делата на ПРБ;

10. обработване на лични данни от охраната и контролиране на достъпа до сградите, както и дейности по съхраняване на документи - обработване на данни от видеонаблюдение и пропускателен режим:

а) съхраняват се в сектор „Техническо обслужване“ /за АГП/ и отдел „Оперативен дежурен център“ в НСлС (за НСлС), като и достъп до тях имат само оторизирани служители. Външната поддръжка няма достъп до данните.

б) записите от видеонаблюдение се съдържат на сървър в АГП, респ. на дискови записващи устройства в НСлС, пазят се 1 месец и се унищожават;

в) вписване в дневник на три имена на посетителите - съхранява се 2 години.

11. обработване на лични данни във връзка със съхраняване на архив:

а) съхраняват се в Служба „Архив“ в специални помещения, пригодени за архивна дейност;

б) при обработването се прилагат изискванията на Закона за Националния архивен фонд и Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции, а сроковете за съхранение са посочени в Номенклатурата на делата на ПРБ.

12. обработване на лични данни във връзка с издаване на удостоверителни документи/удостоверения:

а) съхраняват се в Служба „Регистратура и деловодство“ в Националната следствена служба, Софийската градска прокуратура, окръжните и районните прокуратури;

б) съхранят се в сроковете, посочени в Номенклатурата на делата на ПРБ.

(2) Конкретните мерки по ал. 1 се прилагат за съответните информационни активи в допълнение към мерките по чл. 31.

Контрол по прилагането на техническите и организационните мерки

Чл. 31б. (1) Служителите на ръководни длъжности в АГП, както и в структурите с право на достъп до лични данни при ПРБ следят за прилагането на техническите и организационните мерки и контролират служителите от техните звена относно тяхното спазване.

(2) При неспазване на технически и организационни мерки, описани в тази процедура или при нарушаване функционирането или целостта на средствата за защита на информационните активи, съответните служители на ръководни длъжности вземат всички възможни мерки за отстраняване на несъответствието. В случай че това не е в тяхната компетентност, сигнализират съответните административни ръководители и ръководителите на структурите с право на достъп до лични данни при администратора на лични данни ПРБ за отстраняване на нередностите.

(3) Контрол на достъпа до регистрите се упражнява от административния ръководител или определено от него длъжностно лице.

VIII. ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ (ПОЖАР, НАВОДНЕНИЕ И ДР.)

Чл. 32. (1) При възникване и установяване на инцидент, веднага се докладва на ръководителите на структури по чл. 4, ал. 2 и в зависимост от обстоятелствата, се уведомяват съответните институции.

(2) С наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, ако това е възможно.

(3) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на ръководителите на структури по чл. 4, ал. 2, като това се отразява в дневника по архивиране и възстановяване на данни.

IX. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 33. Лични данни, обработвани от администратора, се предоставят на трети държави и международни организации единствено в изпълнение на задължения по нормативни актове. При необходимост от такова предоставяне се спазват разпоредбите на Глава пета от Регламент (ЕС) 2016/679 и Глава осма, раздел IV от ЗЗЛД.

Чл. 34. (1) Данни, обработвани при осъществяване на дейност по управление на човешки ресурси, могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и др.).

(2) В качеството си на работодател, в случаите и по ред, предвидени в закон, ПРБ чрез ръководителите на структури по чл. 4, ал. 2 предоставят лични данни на служители и магистрати и на определени кредитни институции (например банки), във връзка с изплащането на дължимите възнаграждения на служители, изпълнители по граждански договори, кредитни задължения и др.

Чл. 35. (1) Администраторът ПРБ чрез ръководителите на структури по чл. 4, ал. 2 взема мерки за защита на личните данни в процеса на подготовка, сключване и изпълнение на договорни споразумения с трети лица (контрагенти).

(2) Администраторът чрез ръководителите на структури по чл. 4, ал. 2 сключва писмено споразумение с контрагента по договора и изисква от него да третира личните данни, които ще му станат известни в процеса на изпълнение на договора, като поверителни и да не ги разкрива, освен на служителите си и обработващи подизпълнители и само доколкото това е необходимо за изпълнение на дейностите по договора.

(3) В случаите, когато договорът е със страна, която се явява обработващ по смисъла на ОРЗД, администраторът изисква от контрагента да осигури подходящи мерки за сигурност на личните данни, които ще обработва и в споразумението се предвиждат най-малко следните гаранции:

1. Задължава обработващият да третира всички лични данни, предадени от Администратора или възникнали по време на обработването, като поверителни, като не ги разкрива, освен на служителите си и обработващи подизпълнители и само до колкото това е необходимо за изпълнение на дейностите по договора.
2. Забранява на обработващият да използва от своя страна подизпълнители за обработването на личните данни без изрично писмено разрешение от Администратора.
3. В случаите, когато на обработващия бъде разрешено да превъзложи обработването на лични данни на подизпълнител, обработващият от първо ниво трябва да забрани на подизпълнителя от второ ниво (и по-нататък по веригата) да превъзлага дейността по обработка на данни на подизпълнители без писменото разрешение от Администратора;
4. Договорите с подизпълнители от второ ниво се одобряват, само ако изискват от тях да спазват най-малко същите разпоредби за сигурност и другите изисквания, които се отнасят и до основната организация обработващ.
5. При прекратяването на договор с обработващия или негови подизпълнители, съответните лични данни трябва да бъдат унищожени или върнати на администратора по веригата от подизпълнители.

X. УСЛОВИЯ И РЕД ЗА УНИЩОЖАВАНЕ ИЛИ ИЗТРИВАНЕ НА ЛИЧНИ ДАННИ

Лични данни, които подлежат на унищожаване или изтриване

Чл. 36. (1) На унищожаване или изтриване подлежат лични данни, за които е приложимо едно от следните условия:

а) постигнати са целите, за които са били събрани или обработвани по друг начин;

б) изтекли са сроковете за съхранение и данните трябва да бъдат унищожени или

изтрити с цел спазване на нормативно установено задължение;

в) периодичната проверка относно необходимостта от съхраняване на лични данни не мотивира необходимост от продължаване на съхранението и е предложено унищожаване или изтриване;

г) уважено е правото на изтриване на субекта на данни по чл. 17, пар. 1 от Регламент (ЕС) 2016/679 или по чл. 56, ал. 2 от ЗЗЛД;

д) получено е уведомление по чл. 19 от Регламент (ЕС) 2016/679 или по чл. 56, ал. 10 от ЗЗЛД и личните данни не се обработват за друга цел;

е) личните данни трябва да бъдат изтрити или унищожени съобразно разпоредбите на чл. 25а от ЗЗЛД.

(2) Освен ако не е определено друго, при унищожаване на лични данни в документ на хартиен носител, същите се заличават и в наличните електронни образи на документа, снети съгласно чл. 360ж, ал. 1 от Закона за съдебната власт, респ. в съответния електронен носител, ако документът е бил представен при условията на чл. 360ж, ал. 2 от Закона за съдебната власт. Личните данни се унищожават/изтриват по реда на чл. 37, ал. 4 – когато са на хартиен носител, и на чл. 38, ал. 3 - когато са в електронен формат.

(3) Документи на хартиен носител или в електронен формат могат да се използват като примерни образци на документи в дейността на ПРБ след анонимизиране на личните данни в тях.

Унищожаване на лични данни на хартиен носител

Чл. 37. (1) Унищожаването на лични данни, които се съдържат в документи на хартиен носител, се извършва при спазване на изискванията на Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции /Наредбата/. При спазване на критериите по чл. 47 от Наредбата постоянно действащите експертни комисии в ПРБ описват документите, съдържащи лични данни, за които са налице условия за унищожаване, като неподлежащи на запазване документи в акт за унищожаване съгласно приложение № 7 или Приложение № 7а от Наредбата.

При извършването на преценката се отчита и:

а) значението на документите за целите по чл. 42, ал. 1 от ЗЗЛД, при което документите не се унищожават, а се преразглеждат периодично в съответствие с чл. 46 от ЗЗЛД;

б) историческото, практическото и/или справочното значение на документите за дейността на ПРБ, при което документите не се унищожават, а се запазват в предвидените от нормативен акт или в Номенклатурата на делата на ПРБ срокове, след което оригиналите се архивират в обществен интерес чрез предаването им в съответния държавен архив;

в) значението на документите за установяване, упражняване или защита на правни претенции, които се обработват при спазване на изискванията на Регламент (ЕС) 2016/679 – до постигането на съответните цели.

(2) В съответствие с чл. 49, ал. 1 от Закона за Националния архивен фонд документите от масово-типов характер, неподлежащи на запазване, се описват в акт по ал. 1, който се утвърждава от съответния административен ръководител. Актът се съставя от постоянно действащата експертна комисия съобразно давностните срокове, посочени в закон, и тези, посочени в Номенклатурата на делата на ПРБ. Екземпляр от утвърдения акт

се изпраща в двумесечен срок **преди** унищожаването на документите за сведения в съответния държавен архив.

(3) До унищожаването на документите се вземат всички мерки, за да се гарантира, че личните данни няма да бъдат използвани за други цели и няма да се наруши тяхната сигурност, включително ограничаване на обработването на електронните образи на подлежащите на унищожаване документи по правилата на чл. 38, ал.2.

(4) Унищожаването на документите се извършва след изпълнение на всички изисквания, произтичащи от Закона за Националния архивен фонд и Наредбата, и по начин, непозволяващ изцяло или частично възстановяване или възпроизвеждане на информацията, например нарязване или по друг начин, за което постоянно действащата експертна комисия съставя протокол и го представя на административния ръководител за утвърждаване.

(5) В случай, че унищожаването на документите бъде възложено на външен изпълнител, по отношение на унищожаването той действа в качеството на обработващ лични данни и спрямо него се спазват всички изисквания, произтичащи от чл. 28 от Регламент (ЕС) 2016/679. Обработващият лични данни документира унищожаването и представя протокол.

(6) Протоколите за извършено унищожаване се оформят в сборове от документи, които не се приключват и не се предават в архив. Не се разрешава извършването на поправки и зачеркванията върху протоколите.

(7) След приключване на процедурата по унищожаването на документите на хартиен носител определен/и от административния ръководител служител/и с право на достъп до УИС отбелязва/т в системата, че хартиените им носители са унищожени и предприема/т действия за изтриване на електронните им образи в УИС. При необходимост служителите от дирекция „Информационно обслужване и технологии" в АГП и от направление „Информационно обслужване" в съответните прокуратури оказват техническа помощ и съдействие за програмно изтриване на съответната съвкупност на електронните образи в УИС. Доказването на изтриването става чрез системните дневници (логове) по чл. 38, ал. 4.

(8) Не се допуска изтриване, ако електронните образи на документите са необходими за доказателствени цели, за архивиране в обществен интерес, за научни или исторически изследвания или статистически цели. В тези случаи, в изпълнение на чл. 45, ал. 3 от ЗЗЛД, се прилагат подходящи според целите на обработването мерки за защита, като например: анонимизиране или свеждане на данните до минимум – при научни или исторически изследвания.

Изтриване на лични данни в системи за автоматизирано обработване

Чл. 38. (1) За личните данни, съхранявани в електронен формат, се предприемат действия по изтриване, ако е изпълнено поне едно условие по чл. 36, ал. 1.

(2) Наличието на условие за изтриване се мотивира пред съответния административен ръководител и обработването им се ограничава, като личните данни се маркират по начин, който указва, че не подлежат на операции по по-нататъшно обработване и не могат да се променят. Ограничаването на обработването се осъществява чрез разработена за това функционалност в системата.

(3) Данните се изтриват чрез стандартните средства на операционната система или чрез специализирани софтуерни продукти, по начин, който или изтрива самия

документ/файл, или необратимо анонимизира личните данни в него (изтриване на всички данни, които идентифицират или могат да идентифицират физическите лица). Във всички случаи изтриването на файловете или личните данни се извършва по начин, който не позволява изцяло или частично възстановяване на информацията.

(4) Изтриването се документира чрез системните дневници (логове), които се водят за операциите по изтриване, в съответствие с чл. 63 от ЗЗЛД. Системните дневници (логове) дават възможност за установяване на основанието, датата и часа, както и лицето, направило изтриването.

(5) Системните дневници (логове) се съхраняват за срок не по-кратък от две години, след което се архивират.

Изтриване на лични данни, събирани в резултат на видеонаблюдение

Чл. 39. (1) Лични данни, събирани в резултат на видеонаблюдение, се изтриват автоматично чрез запис на новата информация върху записите с изтекъл срок за съхранение. За целта механизмите за видеонаблюдение се конфигурират по начин, че новозаписаната информация да е записана върху носителя, на който събраните лични данни са с изтекъл срок за съхранение.

(2) При необходимост определен запис да бъде съхранен за по-дълъг период от време, съответният ръководител разпорежда да се направи презапис или да се съхрани на отделен носител, за да не бъде автоматично изтрит. Подлежи на документиране причината, която налага по-дълъг период на съхранение, както и изтриването на записа след отпадане на основанията за неговото съхранение.

Изтриване на лични данни в материални носители за запис

Чл. 40. (1) Записването на лични данни в преносими носители за запис (преносима памет, дискове и други подобни) се допуска по изключение, ако е необходимо за нуждите на работата.

(2) След приключване на дейността, изискваща записа, служителят прехвърля файловете на служебния си компютър и ги изтрива от носителя. В случай, че информацията не може да бъде изтрита от носителя, например поради техническа повреда или естеството на носителя не го позволява, носителят се предава на дирекция „Информационно обслужване и технологии“ за унищожаване по реда на ал. 3.

(3) Записите, които не могат да бъдат изтрити от техните носители, както и носителите, за които е преценено да бъдат извадени от употреба, се унищожават в дирекция „Информационно обслужване и технологии“. Унищожаването се извършва по начин, непозволяващ използването на носителя или на части от него и извличането на остатъчна информация. За унищожаването се съставя протокол по образец и се предава за съхранение в служба “Архив“.

Унищожаване или изтриване на лични данни в резултат на уважаване на право на изтриване на субекта на данни

Чл. 40а. (1) Унищожаване или изтриване на лични данни в резултат на уважаване на право на изтриване на субекта на данни се прилага в случаите по чл. 17, пар. 1 от Регламент (ЕС) 2016/679, когато обработването на лични данни се регулира от този регламент.

(2) При искане за унищожаване или изтриване на лични данни, които се обработват за целите по чл. 42, ал. 1 от ЗЗЛД и се съдържат в съдебно решение, документ или материали по дело, изготвени в наказателно производство, се отчитат разпоредбите на Наказателно-процесуалния кодекс.

(3) В зависимост от носителите им, личните данни по ал. 1 се унищожават или изтриват след влизане в сила на акта, с който е постановено изтриването им. Унищожаването или изтриването се документират.

(4) Получателите на личните данни се уведомяват за извършеното унищожаване или изтриване, с цел предприемане на съответните действия по отношение на съхраняваните от тях екземпляри/копия на личните данни.

Унищожаване или изтриване на лични данни след получено уведомление по чл. 19 от Регламент (ЕС) 2016/679 или по чл. 56, ал. 10 от ЗЗЛД

Чл. 40б. (1) При получено уведомление от друг администратор по чл. 19 от Регламент (ЕС) 2016/679 или по чл. 56, ал. 10 от ЗЗЛД се прави проверка за какви цели се обработват съответните лични данни.

(2) Личните данни се унищожават или изтриват по реда на чл. 37 и чл. 38, но само ако не са необходими за целите по чл. 42, ал. 1 от ЗЗЛД или за други легитимни, конкретни и изрично указани цели в дейността на ПРБ.

Анонимизиране на лични данни в документи, предназначени за достъп от други лица

Чл. 40в. (1) Когато е необходимо да се предостави достъп до лични данни на субекта на данни, но в документите се съдържат данни и за трети лица, за чието предоставяне няма правно основание, съответният административен ръководител в ПРБ, директорът на НСлС, ръководителите на учебни и почивни бази по отношение на съхраняваните в съответните структури лични данни може да разпореди да бъде предоставен достъп след анонимизиране на личните данни на трети лица.

(2) Анонимизирането се извършва чрез обезличаване на идентификаторите на трети лица в копия от документите по ал. 1 и достъпът се предоставя до копието от документите.

Унищожаване или изтриване на лични данни в случаите по чл. 25а от ЗЗЛД

Чл. 40г. (1) Когато лични данни са предоставени от субекта на данни без правно основание по чл. 6, пар. 1 от Регламент (ЕС) 2016/679 или в противоречие с принципите по чл. 5 от същия регламент, в срок от един месец от узнаването документите се връщат на субекта на данни, а ако това е невъзможно или изисква несъразмерно големи усилия, се изтриват или унищожават. Този ред се прилага само по отношение на лични данни, обработвани за цели, различни от целите по чл. 42, ал. 1 от ЗЗЛД.

(2) Длъжностното лице по защита на данните, при необходимост, дава становище по случаите, в които се изисква унищожаване или изтриване в съответствие с чл. 25а от ЗЗЛД.

(3) При необходимост от изтриване или унищожаване, съответният административен ръководител организира документиране на съответната причина и предприетите действия по изтриване или унищожаване.

XI. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл. 41. Всяко физическо лице има право на безплатен достъп до отнасящи се за него лични данни на основание и по реда на Регламент (ЕС) 2016/679 или на ЗЗЛД и в зависимост от целите на обработването.

Чл. 42. (1) Правото на достъп се осъществява с писмено заявление до администратора. Заявлението се подава лично или от изрично упълномощено лице, което се прилага към заявлението. Заявление може да бъде отправено и чрез ръководителите на структурите по чл. 4, ал. 2, както и по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги (ЗЕДЕУС), Закона за електронното управление и Закона за електронната идентификация.

(2) Информацията може да бъде предоставена под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице. Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон. АЛД е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

(3) АЛД разглежда заявлението за предоставяне на пълна или частична информация, и се произнася в съответните срокове, произтичащи от Регламент (ЕС) 2016/679 или ЗЗЛД според целта на обработването.

(4) АЛД отказва достъп до лични данни, когато те не съществуват или предоставянето им е забранено със закон или когато са налице други нормативни ограничения.

(5) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, АЛД е длъжен да предостави на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

(6) Физическото лице има право по всяко време да поиска от АЛД да заличи или коригира негови лични данни, обработването на които не отговарят на изискванията на ЗЗЛД.

(7) Когато информацията, съдържа данни, представляващи класифицирана информация, се прилага редът по ЗЗКИ.

Чл. 43. (1) Във връзка с обработването на лични данни за целите по чл. 1, ал. 2 субектът на данни има следните права:

1. Да получи потвърждение дали се обработват лични данни, които го засягат, и ако това е така, да получи достъп до тях, както и информация за обстоятелствата по чл. 15, ал. 1, т. 1-4 и чл. 15, ал. 2, т. 1, обработваните категории лични данни и личните данни, които са в процес на обработване, както и всякаква налична информация за техния произход, освен когато тази информация е защитена от закон тайна.

2. Да поиска коригиране на неточните лични данни, свързани с него, както и допълване на непълните лични данни. При коригиране, администраторът съобщава на компетентния орган, от който е получил неточните лични данни;

3. Да поиска изтриване на личните данни, които го засягат, когато обработването нарушава разпоредбите на ЗЗЛД. Личните данни не се изтриват, но обработването им се ограничава, когато:

- точността на личните данни се оспорва от субекта на данните и това не може да се провери.

Преди премахването на ограничаването на обработването, администраторът е длъжен да информира субекта на данните;

- личните данни трябва да се запазят за доказателствени цели.

При извършени корекции, допълвания, изтривания или ограничаване на обработването, администраторът уведомява получателите на личните данни.

4. Да бъде писмено информиран, когато администраторът отказва да коригира, допълни, изтрие или ограничи обработването на лични данни в случаите по чл. 15, ал. 3.

5. Да бъде информиран от администратора за правото да подаде жалба до Инспектората, както и да търси защита по съдебен ред.

(2) Информацията се предоставя в двумесечен срок от получаване на искането, който може да се удължи с още един месец поради сложността или броя на исканията;

(3) Упражняването на правата по чл. 15, ал. 1-2 и чл. 42, ал. 1, когато личните данни се съдържат в документ или материали по дело, изготвени по наказателно производство, не може да засяга или да противоречи на разпоредбите на НПК.

XII. УПРАВЛЕНИЕ НА ЗАЯВЛЕНИЯТА (ИСКАНИЯТА) ОТ СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл. 44. ПРБ, в качеството си на администратор на лични данни, чрез ръководителите на структури по чл. 4, ал. 2, организира и отговаря за обработването на всички заявления (искания) на субекти на данни, които са резултат от упражняване на правата, дадени им съгласно ОРЗД и ЗЗЛД.

Чл. 45. (1) При отправянето на искане субектът на данни предявява заявлението в свободна форма или като използва образеца на формуляра, предоставен от администратора и публикуван на интернет страницата му.

(2) Заявлението (искането) трябва да съдържа реквизитите, които са посочени в чл. 37в от Закона за защита на личните данни.

(3) При подаването на заявление от упълномощено лице към заявлението се прилага и пълномощното.

Чл. 46. (1) При отправяне на заявление (искане) се спазват следните правила:

1. Субектът на данните може да поиска достъп до всички негови лични данни, обработвани от администратора, без да указва конкретен вид – прилага се при съобразяване с целите на обработване на данните;

2. Субектът на данните предоставя на администратора посочените в чл. 37в от ЗЗЛД данни за самоличността си, които да го идентифицират сигурно и еднозначно;

3. Администраторът задължително проверява идентификационните данни, за да се увери, че искането е подадено от субекта, когото данните идентифицират;

4. Заявление може да се подаде и по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация.

5. Заявление може да се подаде и чрез действия в потребителския интерфейс на информационната система, която обработва данните, след като лицето е идентифицирано със съответните за информационната система средства за идентификация.

6. Заявлението се завежда в деловодната система на ПРБ.

(2) Администраторът разглежда искането и излиза с решение да се удовлетвори или не заявлението на субекта на данни относно упражняването на негови права.

(3) Администраторът предоставя исканата информация и отговаря на исканията на субекта на данните в рамките най-късно на един месец (съответно два месеца при обработване за целите по чл. 1, ал. 2) от датата на получаване на заявлението (искането) за достъп. При необходимост този срок може да бъде удължен с още два месеца (съответно един месец), като се взема предвид сложността и броя на исканията (заявленията). Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец (съответно два месеца) от получаване на заявлението (искането), като посочва и причините за забавянето.

(4) Когато заявлението (искането) е за достъп до информация, при предаването на копие от информацията администраторът, подпомогнат от длъжностното лице по защита на личните данни, извършва обработване на данните с цел отстраняване на евентуална идентификационна информация за трети лица.

(5) Идентифицирането (търсенето) на личните данни се извършва във всички хранилища на данни и всички съответни системи за архивиране, включително всички архивирани файлове (компютъризирани или хартиени архиви) и всички папки на електронната поща и техните архиви.

Чл. 47. (1) Отговорът на заявлението се съобщава писмено на заявителя, лично срещу подпис.

(2) Когато субектът на данни подава заявление (искане) с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

(3) В случай, че отговорът на заявлението съдържа лични данни, информацията се съобщава на субекта на лични данни лично, след проверка на самоличността и срещу подпис.

Чл. 48. (1) В случай на заявление (искане) от субекта на данни за „получаване на достъп до данните", наред с осигуряването на това право, например чрез предоставяне на копие на данните, при съобразяване с целите, за които данните се обработват, администраторът изпраща на субекта и следната информация:

1. целите на обработването;

2. съответните категории лични данни;

3. получателите или категориите получатели на личните данни (ако има такива);

4. информация относно намерението на администратора да предаде данните на трета държава или на международна организация, както и наличието на гаранции за защита на данните;

5. срока, за който администраторът ще съхранява личните данни, а ако това е невъзможно - критериите, използвани за определяне на този срок;

6. правото му да се изиска от администратора коригиране или изтриване на неговите лични данни, както и правата му на ограничаване на обработването, на възражение срещу обработването, както и на преносимост на данните;

7. правото на жалба до надзорния орган;

8. когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

9. наличие на автоматизирано вземане на решения, включително профилиране, както и предвидените последствия от това обработване за субекта на данните.

(2) При заявление (искане) на субекта на данни за коригиране, изтриване, ограничаване или при възражение по отношение на обработваните лични данни длъжностното лице по защита на личните данни, а при обработване на личните данни за целите по чл. 1, ал. 2 - ръководителите на структурите с право на достъп по чл. 4, ал. 2, преценяват всяко от тези искания (извън искането за достъп до данни) с оглед основателността на правото на субекта и наличието на други законови изисквания за неговото удовлетворяване.

(3) ДЛЗД съдейства, при необходимост, на администратора като го уведомява за преценката си относно основателността на исканията, с които субектите упражняват правата си.

Чл. 49. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, длъжностното лице по защита на личните данни може:

1. да предложи на ръководството на администратора да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията;

2. да предложи на ръководството на администратора да откаже да предприеме действия по искането (заявлението);

Чл. 50. (1) Длъжностното лице по защита на личните данни и ръководителите на структури по чл. 4, ал. 2 поддържат „Дневник на исканията (заявленията) от субекти на данните".

(2) В Дневника на исканията (заявленията) от субекти на данните се вписват датата, идентифициращата информация и всички други важни за разглеждане на искането данни, както и информация за подадения към субекта отговор на искането за достъп.

Чл. 51. Ръководителите на структурите с право на достъп по чл. 4, ал. 2 създават подходящи процедури, които да определят начините и средствата за изпълнение на задълженията по управление на заявленията за упражняване на права от субектите на данни в структурите на ПРБ.

XIII. ОБУЧЕНИЕ НА СЛУЖИТЕЛИТЕ

Чл. 52. (1) Ръководителите по чл. 4, ал. 3 възлагат на служителите задължения по защита на данните във връзка с настоящите правила за обработване на личните данни.

(2) Длъжностното лице по защита на личните данни съдейства на ръководителите по чл. 4, ал. 3 за запознаване на прокурорите, следователите и служителите относно значението на защитата на данните в изпълнението на преките им задължения чрез разяснения, становища или разработване на наръчници.

(3) Служителите преминават конкретно обучение за обработване на лични данни, свързани с техните постоянни служебни/трудови задължения и отговорности в съответствие с настоящите правила.

(4) Служителите подлежат на обучение относно процедурите при постъпили за разглеждане искания и възражения от субекти на данните, свързани със защитата на личните данни и обработването на лични данни, съгласно настоящите правила.

(5) Длъжностното лице по защита на личните данни трябва да се увери, че всички служители, които имат текущи задължения, свързани с лични данни и операции по обработване, както и тези с редовен достъп до лични данни, са запознати с изискванията за защита на личните данни.

Чл. 53. (1) Всеки новоназначен служител, чиято длъжностна характеристика е свързана с обработването на лични данни, се запознава с Политиката за защита на личните данни на ПРБ и Правила за мерките и средствата за защита на личните данни, обработвани в ПРБ, което се удостоверява с подписване на декларация при назначаване.

(2) Отговорност за изпълнението на задължението по ал. 1 носят съдебните служители, изпълняващи функции по направление „Човешки ресурси".

Чл. 54. Веднъж годишно администраторът, с помощта на ДЛЗЛД, организира обучение на служителите, което включва и запознаване с евентуални нови изисквания относно защитата на личните данни.

Чл. 55. Длъжностното лице по защита на личните данни документира всяко проведено обучение в дневник.

Преходни и Заключителни разпоредби

(изм. със Заповед № РД-02-29 от 23.11.2023 г. на главния прокурор)

§1. Контрол по изпълнението на настоящите правила се осъществява от главния прокурор или определен от него заместник на главния прокурор.

§ 2. Тези правила влизат в сила от датата на утвърждаването й, с изключение на разпоредбата на чл. 38, ал. 3, която влиза в сила от 1 февруари 2024 г.