ПРОКУРАТУРА НА РЕПУБЛИКА БЪЛГАРИЯ

ГЛАВЕН ПРОКУРОР

ЗАПОВЕД

№ РД-02-30/23.11.2023

ОТНОСНО: Утвърждаване на Политика за защита на личните данни в Прокуратурата на Република България

На основание чл. 138, ал. 1, т. 1 от Закона за съдебната власт, чл. 24, т. 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 95/46ЕО (Общ регламент относно защитата на данните)

ЗАПОВЯДВАМ:

1. Отменям Политика за защита на личните данни в Прокуратурата на Република България, утвърдена със Заповед № РД-02-16/28.09.2020 г., изм. със Заповед № 02-27/17.12.2021 г. на главния прокурор.

2. Утвърждавам Политика за защита на личните данни в Прокуратурата на Република България.

3. Заповедта да се публикува на ведомствения информационен сайт на ПРБ.

И.Ф. ГЛАВЕН ПРОКУРОР
НА РЕПУБЛИКА БЪЛГАРИЯ:

БОРИСЛАВ САРАФОВ

София 1000, бул. „Витоша“ № 2, тел. 02/92 19 601, факс: 02/989 01 10, e-mail: office_gp@prb.bg

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ В ПРОКУРАТУРАТА НА РЕПУБЛИКА БЪЛГАРИЯ

I. Въведение

1. Общ регламент относно защита на личните данни

Регламент (ЕС) 2016/679 (Общ регламент относно защита на данните) има пряко действие в страните-членки на ЕС. Неговата цел е да защитава "правата и свободите" на физическите лица и да се гарантира, че личните данни не се обработват без тяхно знание, и когато е възможно, че се обработва с тяхно съгласие.

С Директива (ЕС) 2016/680 на Европейския парламент и на съвета от 27 април 2016 г. се установяват правилата във връзка със защитата на физическите лица по отношение на обработването на лични данни от компетентните органи за целите на предотвратяването, разследването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазване от заплахи за обществената сигурност и тяхното предотвратяване. Разпоредбите на Директивата са транспонирани в българското законодателство като в глава осма на Закона за защита на личните данни се установяват правилата за защита на личните данни, прилагани в хода на полицейската и наказателната дейност.

В ОРЗД последователно е проведена идеята за изключване на органите на съдебната власт от приложното поле на регламента при изпълнение на съдебните им функции.

ОРЗД не се прилага за обработване на лични данни за целите на предотвратяването, разкриването или наказателното преследване на престъпления или изпълнение на наложени наказания, за предпазването от и предотвратяване на заплахи за обществената сигурност.

Прокуратурата на Република България има утвърдени „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. на главния прокурор, наричани по-долу „Вътрешни правила на ПРБ“.

2. Обхват на Общия регламент относно защита на данните

Материален обхват – Общият регламент се прилага за обработването на

лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (например ръчно и на хартия), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Териториален обхват – правилата на Общия Регламент важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност. Прилагат се и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС.

3. Приложими правни изисквания според целите на обработването

3.1. Личните данни, които се обработват в ПРБ за целите по чл. 42, ал. 1 от Закона за защита на личните данни (ЗЗЛД) – предотвратяване, разследване, разкриване или наказателно преследване на престъпления или изпълнението на наказания, включително предпазване от заплахи за обществения ред и сигурност и тяхното предотвратяване, се обработват, респ. съхраняват, унищожават или изтриват в съответствие с изискванията на Глава осма от ЗЗЛД.

3.2. Личните данни, обработвани за цели, различни от целите по чл. 42, ал. 1 от ЗЗЛД, се унищожават или изтриват в съответствие с 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). Обработването за цели, различни от тези по чл. 42, ал. 1 от ЗЗЛД, обхваща:

3.2.1. обработването на лични данни, свързано с изпълнение на правомощията на ПРБ в предвидените със закон случаи да участва в граждански и административни дела и да предприема действия за отмяна на незаконосъобразни актове;

3.2.2. обработването на лични данни при управлението на човешките ресурси;

3.2.3. обработване на лични данни при осъществяването на финансово-стопанската дейност, както и обработването на лични данни за осъществяване на контролиран достъп до определени места- в съдебните сгради или охраната на стопанисваните имоти;

3.2.4. обработване на лични данни при изпълнение на нормативни изисквания по Закона за достъп до обществена информация, Закона за обществените поръчки и други нормативни актове, при обработване на лични данни, съдържащи се в предложения и сигнали по Административнопроцесуалния кодекс и по Закона за защита на лицата, подаващи сигнали или публично оповестяващи

информация за нарушения за деяния, които не представляват престъпление, в искания за достъп до преписки, подадени от лица със законен интерес и други;
3.2.5. обработване на лични данни в дейността на учебните и почивните бази на ПРБ;
3.2.6. обработване на лични данни във връзка с издаване на удостоверителни документи/удостоверения за наличие или липса на повдигнати обвинения по неприключени наказателни производства спрямо конкретно лице;
3.2.7. други конкретни, изрично указани и легитимни цели извън целите по чл. 42, ал. 1 от ЗЗЛД.

4. Понятия

4.1. ***„Лични данни"*** - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице, както и всяка друга информация, която се определя от приложимото право като лични данни;

4.2. ***„Специални (чувствителни) категории лични данни"*** – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация , както и всички други лични данни, които се определят от приложимото право като специални.

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

4.4. ***„Администратор"*** - всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други

определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

4.5. *„Субект на данните“* – всяко живо физическо лице, което е предмет на личните данни, съхранявани от Администратора.

4.6. *„Съгласие на субекта на данните"* - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

4.7. *„Дете“* – Общият Регламент определя дете като всеки на възраст под 16 години, въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си;

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

4.9. *„Нарушение на сигурността на лични данни"* - нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

4.10. *„Получател"* - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

4.11. *„Трета страна“* – всяко физическо или юридическо лице, публичен

орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

4.12. *„Документ“* означава всяка информация, която съдържа лични данни, независимо на какъв информационен носител (на хартиен носител или в електронен формат, звукозапис, видео- или аудио-визуален запис), обработвани в Прокуратурата на Република България;

4.13. *„Електронен формат“* включва носители на данни като дискови носители (компютри, USB флаш памети, външни дискове и др.), оптични носители (DVD, CD и др.) и магнитни носители (дискети);

4.14. *„Унищожаване“* е необратимо физическо разрушаване на материалния носител на информация;

4.15. *„Изтриване“* е необратимо заличаване на информацията от съответния носител;

4.16. *„Ограничаване на обработването“* е понятието по чл. 4, т. 3 от Регламент (ЕС) 2016/679 и означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще. Методите за ограничаване на обработването могат да включват: временно преместване на избраните лични данни в друга система за обработване, прекратяване на достъпа на ползвателите до тях, или временно премахване на публикуваните данни от уебсайт. В автоматизираните регистри на лични данни ограничаването на обработването следва да бъде осигурено с технически средства, така че личните данни да не подлежат на операции по по-нататъшно обработване и да не могат да се променят. Фактът, че обработването на лични данни е ограничено, следва да бъде ясно посочен в системата.

II. Декларация относно политиката по защита на личните данни

1. Прокуратурата на Република България се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на "правата и свободите" на лицата, чиито лични данни се събират и обработват съгласно Общия регламент за защита на данните.

2. Прокуратурата на Република България се задължава да осигури

съответствието на всички дейности, които извършва, по събиране и обработване на лични данни, съгласно изискванията на ОРЗД и ЗЗЛД.

3. Настоящата политика обхваща дейностите по обработване на лични данни при осъществяване на работата (преди всичко) на администрацията на Прокуратурата на Република България.

Настоящата политика НЕ обхваща дейности по обработване на лични данни, които са извършват при изпълнение на правомощията на прокуратурата като орган на съдебната власт.

4. Прокуратурата на Република България води Регистър на дейностите по обработване *(Приложение № 1)*. Воденето на регистъра е възложено на Длъжностното лице по защита на данните и то отговаря за въвеждането в този регистър на всякакви промени в дейностите на Прокуратурата на Република България, както и на всички други допълнителни изисквания, в т.ч. оценки на въздействието върху защитата на данните. Този регистър трябва да бъде на разположение по искане на надзорния орган.

5. Тази политика се прилага за всички служители *(Приложение № 2)* на ПРБ, както и за обработващите и членовете на техния персонал. Всяко нарушение на Общия регламент се разглежда като нарушение на трудовата дисциплина.

6. Трети страни, които работят с или за ПРБ, в т.ч. партньори, външни доставчици и др. *(Приложение № 3)*, както и които имат или могат да имат достъп до личните данни, обработвани в ПРБ, са длъжни да се запознаят и съобразят с тази политика. ПРБ е длъжна да сключи споразумение за поверителност на данните с всяка трета страна, на която предоставя достъп до личните данни, освен ако обработването не се изисква от правото на ЕС или от българското право.

7. ПРБ може да извършва проверки на спазването на наложените със споразуменията по т. 6 задължения.

III. Задължения и отговорности по Регламент (ЕС) 2016/679

1. Прокуратурата на Република България като администратор на данни съгласно Регламент (ЕС) 2016/679 носи отговорността и рисковете от евентуално несъответствие с изискванията на ОРЗД, включително отговорността за разработване и насърчаване на добри практики в областта на обработване на личните данни в рамките на организацията.

2. Обработващ лични данни е всяко лице извън структурата на ПРБ, което обработва пряко личните данни от името на ПРБ - съхранява, дигитализира, каталогизира и т.н. цялата информация.

3. Длъжностното лице по защита на данните взема участие при обсъждането на въпроси, свързани със защита на личните данни, и съветва ръководството на ПРБ за изграждане и доказване на съответствието със законодателството в областта на защита на данните и добрите практики.

4. ДЛЗД е длъжно да съветва и информира администратора за прилагането на ОРЗД и други актове от вътрешното и европейското законодателство в областта на защита на личните данни, съобразно задълженията си и съгласно изискванията на ОРЗД, включително да следи за прилагането на тази политика. Информирането може да се извършва и чрез публикуване на разяснителни материали или становища в специално създадена рубрика/раздел във вътрешно-ведомствената страница на ПРБ, посветена на защитата на личните данни.

5. ДЛЗД има и специфични задължения по ОРЗД – информира се за постъпили искания на субектите на данни (виж „Процедура за управление на исканията от субектите“ - *Приложение № 4)*, както и за всички открити случаи на нарушение сигурността на личните данни (виж. Процедура по уведомяване за нарушение на сигурността на личните данни - *Приложение № 5)* и е контактна точка за служителите на ПРБ, които искат разяснения по всеки аспект на спазването на защитата на данните. ДЛЗД е лицето за контакт и пред надзорния орган.

6. Спазването на законодателството за защита на данните е отговорност на всички магистрати и служители, които обработват лични данни, съобразно задълженията си.

7. Политиката за обучение на ПРБ (Политика за провеждане на обучение - *Приложение № 6)* определя специфичните изисквания за обучение и осведомяване във връзка с конкретните роли на служителите.

IV. Принципи за защита на данните

Цялото обработване на лични данни се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиките и процедурите на ПРБ имат за цел да гарантират спазването на тези принципи.

1. Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно.

Законосъобразно идентифициране на законна основа, преди обработване на лични данни. Това са т. нар "основания за обработване", например „съгласие“. Съгласието на субекта е едно от основанията за обработване на личните данни – *Приложение № 7*. Такова може да бъде също изпълнение на договор или

законен интерес на ПРБ, в които случаи съгласие не е нужно да бъда давано.

Добросъвестно - за да може обработването да бъде добросъвестно, ПРБ трябва да предостави определена информация на субектите на данни, необходима във всеки конкретен случай и за всяка конкретна цел, по разбираем, кратък и достъпен за субекта на данни начин. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

Прозрачно – Регламент (ЕС) 2016/679 поставя изисквания относно това, каква информация трябва да бъде предоставена на разположение на субектите на данни, която е обхваната от принципа за "прозрачност", регламентиран в членове 12, 13 и 14 от ОРЗД. Съгласно цитираните разпоредби на ОРЗД, информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език, т.е. декларациите за поверителност, които се подписват от субектите на данни, трябва да бъдат подробни и конкретни, разбираеми и достъпни.

Правилата за уведомяване на субекта на данни са определени в Процедура за прозрачност при обработката на лични данни *(Приложение № 8)* и уведомлението се записва в Декларация за поверителност/Уведомление за поверително третиране на личните данни) (*Приложение № 9*).

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- данни, които идентифицират ПРБ и данните за контакт;
- контактите на ДЛЗД;
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на

данните;

- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

2. Лични данни могат се събират само за конкретни, изрично указани и законни цели.

Данните, получени за конкретни цели, следва да се събират и обработват само за тези цели, които съответстват на дейностите по обработване, включени в Регистъра на дейностите по обработване на данни (чл. 30 ОРЗД) на ПРБ (виж Приложение № 8 – Процедура за прозрачност при обработка на лични данни).

3. Личните данни, които администраторът събира, трябва да бъдат ограничени до това, което е необходимо за съответната цел на обработване *(принцип на минимизиране на данните, които могат да бъдат обработвани за конкретния субект)*:

- ДЛЗД и ръководителите на структури с право на достъп или определени от тях лица следят служителите да са запознати с този принцип, както и при нови дейности за обработване на лични данни да се събира само тази информация, която е строго необходимо за целта на обработване.

- Всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в новите информационни системи, трябва да включват декларация за добросъвестно обработване или връзка към Уведомление за поверително третиране на личните данни (Декларация за поверителност) *(Приложение № 9)*.

- Длъжностното лице по защита на данните и лицата, определени от ръководителите на структурите с право на достъп при адмнинистратора имат задължението да инициират пред ръководството на администратора извършването на периодични проверки, поне веднъж годишно, които да гарантират, че събраните данни продължават да бъдат адекватни, релевантни и не са прекомерни (Процедура за оценка на въздействието върху защитата на данните *(Приложение № 10)*.

4. Личните данни трябва да бъдат точни и актуални във всеки един момент, и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.

- Данните, които се съхраняват от администратора на данни, трябва да бъдат преглеждани и актуализирани при необходимост. Не трябва да се

съхраняват данни, в случаите, когато има вероятност да не са точни.

• Длъжностното лице за защита на данните и ръководителите на структури с право на достъп до данни при администратора трябва да следят за предприемането на мерки, които да гарантират, че целият персонал е обучен в значението на събирането на точни данни и поддържането им.

• От служителите се изисква, да уведомяват ръководителите на съответните административни структури с право на достъп до лични данни при администратора за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на ръководителите на съответните структури е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.

• Длъжностното лице по защита на данните и отговорните за защитата на данните служители, определени от ръководителите на структурните звена с право на достъп до данни следят за наличието на подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени, други относими фактори.

• Най-малко веднъж годишно административните ръководители на прокуратури и Длъжностното лице по защита на данните инициират преглед на сроковете на съхранение на всички лични данни, обработвани в ПРБ.

Въз основа на инвентаризацията на данните се идентифицират всички данни, които вече не се изискват в контекста на съответната цел. Тези данни надеждно се унищожават в съответствие с процедурите и правилата на администратора.

• Ръководителите на структурни звена с право на достъп до лични данни и Длъжностното лице по защита на данните следят за предоставянето на отговори на искания за корекция на данни в рамките на един месец (Процедура за управление на исканията от субектите - *Приложение № 4).* Този срок може да бъде удължен с още два месеца с оглед на сложността и броя на исканията. При отказ, субектът на данните се уведомява за мотивите за отказа и се информира за правото му да подаде жалба пред надзорния орган и да потърси правна защита.

• Ръководителите на структурни звена с право на достъп до лични данни следва да информират всички трети страни, на които са

предоставени неточни или остарели лични данни, че информацията е неточна или остаряла и да не се използва за вземане на решения относно субектите на данни, както и да препраща всяка корекция на лични данни към третите страни, където това е необходимо.

5. Личните данни трябва да се съхраняват в такава форма, която позволява субектът на данните да бъде идентифициран за периода, необходим за обработването.

- Когато личните данни се запазват след срока на обработването, те ще бъдат съхранявани по подходящ начин (минимизирани, криптирани, псевдонимизирани), за да се защити самоличността на субекта на данните в случай на нарушение на данните.
- Лични данни се пазят в съответствие с Вътрешните правила на ПРБ и след като е преминал срокът им на съхранение, те трябва да бъдат надеждно унищожени *(Приложение № 11)*.
- Всяко запазване на данни, което надхвърля срока на съхранение, изисква съответна ясно определена обосновка с изискванията на законодателството за защита на данните.

6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност и съгласно правилата относно техническите и организационни мерки за защита на ПРБ.

При извършването на оценка на въздействието върху защитата на данните, когато такава се налага, се взимат предвид всички обстоятелства, свързани с операциите по обработване на данни от ПРБ.

Във всеки конкретен случай, когато има нарушение на защитата на лични данни, се извърши оценка на риска и при отчитане на висок риск да уведоми надзорния орган и/или субекта на данни *(Приложение № 10)*. При съобразяване на риска в конкретния случай, Длъжностното лице по защита на данните трябва да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физическите лица, ако възникне нарушение на сигурността, всяка вероятна вреда за репутацията на ПРБ, включително евентуална загуба на доверие на гражданите и др.

Гарантирането на сигурността на личните данни е свързана и с предприемането на подходящи технически мерки, които могат да включват:

- Защита с парола;
- Автоматично заключване на бездействащи работни станции в мрежата;
- Антивирусен софтуер и защитни стени;

• Правата за достъп, основани на роли,

• Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;

• Сигурност на локални и широкообхватни мрежи;

• Технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране;

При оценяването на подходящите организационни мерки се съобразяват:

• Нивата на подходящо обучение в ПРБ;

• Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);

• Включването на защитата на данните в трудовите договори;

• Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;

• Редовна проверка на персонала за спазване на съответните стандарти за сигурност;

• Контрол на физическия достъп до електронни и хартиено базирани записи;

• Приемането на политика на „чисто работно място“;

• Съхраняване на хартия на базата данни в заключващи се шкафове;

• Ограничаване на използването на портативни електронни устройства извън работното място;

• Ограничаване на използването от служителите на лични устройства на работното място;

• Приемане на ясни правила за създаване и ползване на пароли;

• Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

При преценката за подходящи мерки се вземат предвид идентифицираните рискове за лични данни, както и възможността за нанасяне на вреди на лицата, чиито данни се обработват.

7. Спазване на принципа на отчетност.

Регламент (ЕС) 2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност в чл. 5, пар. 2 изисква от администратора да докаже, че спазва

останалите принципите в ОРЗД и изрично заявява, че това е негова отговорност.

Прокуратурата на Република България доказва спазването на принципите за защита на данните чрез прилагане на политики и процедури по защита на данните, които да гарантират прилагането на политиките, както и като внедрява подходящи технически и организационни мерки включително и чрез приемане на техники по защита на данните на етапа на проектирането и защита на данните по подразбиране, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и т.н.

V.Права на субектите на данни

1. Съгласно ОРЗД субектът на данни има следните права по отношение на обработването на личните му данни:

- Да получи информация за личните данни, свързани с него, които се обработват от администратора, и за целта, за която се обработват, включително да получи достъп до данните, както и информация кои са получателите на тези данни и третите страни, на които данните се предават;
- Да поиска копие от своите лични данни от администратора;
- Да иска от администратора коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;
- Да изиска от администратора изтриване на лични данни (право „да бъдеш забравен");
- Да иска от ПРБ ограничаване на обработването на лични данни като в този случай данните само се съхранявант, без да се обработват по друг начин;
- Да направи възражение срещу обработване на негови лични данни;
- Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг.
- Да се обърне с жалба до надзорен орган, ако смята, че някоя от разпоредбите на ОРЗД е нарушена;
- Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора *(Приложение №*

12);

- Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие.

2. ПРБ осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

- Субектите на данни могат да направят искания за достъп до данни, както е описано в процедурата за Процедура за управление на исканията от субектите *(Приложение № 4)*; тази процедура също така описва как Администраторът ще гарантира, че отговора на искането на субекта на данни отговаря на изискванията на Общия регламент.
- Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, ръководител на структурно звено с право на достъп до данни може или да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията, комуникацията или предприемането на исканите действия, или да откаже да предприеме действия по искането.
- Субектите на данни имат право да подават възражения, свързани с обработването на личните им данни. Обработването на искане от субекта на данни и подаването на възражения от страна на субекта на данни, се извършва в съответствие с Процедура за начините на комуникация при жалби и искания от субекта на данни *(Приложение № 13)*. Жалбите могат да се подават направо до надзорния орган, като компетентният за това орган в България е Комисия за защита на личните данни, адрес: гр. София 1592, бул. „Проф. Цветан Лазаров" № 2 (www.cpdp.bg). Правото на жалба на субектите на данни във връзка с обработването на техните данни за целите на наказателното преследване и изпълнението на наказания се упражнява чрез подаването й до надзорния орган Инспекторат към Висшия съдебен съвет: гр. София, п.к. 1000, ул. "Георг Вашингтон" №17, тел. деловодство - 02 9057550, факс: 02 9057503, ivss@inspectoratvss.bg, http://www.inspectoratvss.bg/.

VI. Съгласие

1. ПРБ, в качеството си на администратор на лични данни, в своята дейност по обработване на лични данни се ръководи от законовото положение, че съгласието на субекта на данните е едно от правните основания за обработването на лични данни и попада в обхвата на настоящите правила.

Администраторът използва съгласието като основание за обработване на данни, когато данните не се обработват на друго правно основание от посочените в чл. 6 на ОРЗД.

2. Под „съгласие“ следва да се разбира всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени. Субектът на данните може да оттегли своето съгласие по всяко време. Съгласие на субекта на лични данни се изисква винаги, когато не съществува алтернативно правно основание за обработването.

3.Валидно "съгласие" е налице само в случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

4. Наличие на съгласие не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. ПРБ трябва да може да докаже, че е получено съгласие за дейностите по обработване.

5. За специални категории данни трябва да се получи изрично писмено съгласие *(Приложение № 7)* на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.

6. Когато се обработват лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т. н.). За България, според чл. 25в от ЗЗЛД това изискване се прилага за деца на възраст под 14 години.

VII. Сигурност на данните

1. Сигурността на данните в ПРБ се основава на изпълнението на техническите и организационни мерки, залегнали във Вътрешните правила на ПРБ, правилата относно мрежовата и информационната сигурност на комуникационните и информационните системи, деловодната дейност и документооборота, физическия достъп до помещенията, в които се обработват лични данни, както и правилата относно изтриването и унищожаването на лични данни.

2. Служителите на ПРБ, които съгласно длъжностните си характеристики имат задължение да обработват определени лични данни от името на администратора, са длъжни да осигурят сигурността при обработването и

съхраняването на данните от тяхна страна, както и да не разкриват данните на трети страни, освен ако Администраторът-ПРБ не е дал такива права на тази трета страна за достъп до данните (например, въз основа на договор/клауза за поверителност – *Приложение № 14 и Приложение № 15*).

3. Личните данни или част от тях трябва да бъдат достъпни само за тези, които имат задължение да ги обработват/съхраняват, като достъпът може да бъде предоставен само в съответствие с изградените правила за контрол на достъпа. Всички лични данни трябва да се обработват и съхраняват като се вземат предвид разпоредбите на Вътрешните правила на ПРБ.

4 ПРБ се поддържат организационни и технически мерки, които гарантират, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизирани служители.

Всички служители, които обработват лични данни преминават обучение за спазване на организационните и технически мерки за достъп до лични данни преди да им бъде предоставен достъп до информация от всякакъв вид. Обучението се провежда съгласно Политиката за провеждане на обучение *(Приложение № 6)*.

5. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат извеждани от определените офисни помещения без изрично разрешение.

Тяхната обработка, движение и архивиране трябва да бъдат съобразени с правилата относно деловодната дейност и документооборота в ПРБ.

Унищожаването на чернови и копия на документи се извършва по ред, определен от ръководителите на структурните звена с право на достъп при администратора.

6. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с въведените за това правила. Записите на хартиен носител, за които е изтекъл срокът за съхранение, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени.

7. Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обектите на администратора.

VIII. Разкриване на данни

1. ПРБ осигурява условия, при които личните данни не се разкриват на

неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители трябва да бъдат предпазливи, когато се поиска от тях да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността, извършвана от организацията.

На служителите се извършва специално обучение и периодични инструктажи, в съответствие с Политиката за провеждане на обучение *(Приложение № 6*), с цел да се избегне рискът от такова нарушение.

2. Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и, при необходимост, разкриванията на данни се координират с Длъжностното лице за защита на данните.

3. Лични данни се предоставят на компетентните публични власти при и по повод упражняване на техните властнически правомощия.

IX. Съхраняване и унищожаване на данните

1. ПРБ съхранява и заличава лични данни съгласно правилата относно мерките и средствата за защита на личните данни.

2. ПРБ не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период, отколкото е необходимо, по отношение на целите, за които са били събрани данните.

3. ПРБ може да съхранява данни за по-дълги периоди, единствено когато тяхното обработването е за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

4.**Срок за съхранение на личните данни**

4.1. При определяне на сроковете за съхранение на лични данни се прилагат сроковете, предвидени в съответните нормативни актове и в Номенклатурата на делата на ПРБ по чл. 43 от Закона за Националния архивен фонд /ЗНАФ/.

4.2. За личните данни, обработвани за целите по чл. 42, ал. 1 от ЗЗЛД, за които не е установен срок за съхранение в нормативен акт или в Номенклатурата на делата на ПРБ, се извършва периодична проверка на необходимостта от съхранението им в съответствие с чл. 46 от ЗЗЛД.

4.3. Периодичната проверка по т. 4.2 се прилага и за лични данни, чието съхраняване е постановено, за да се запазят за доказателствени цели, за целите на архивирането в обществен интерес, за научни или исторически изследвания

или за статистически цели.

4.4. Периодичната проверка по т. 4.2 и 4.3 се извършва на всеки 3 години и се организира от лицата, определени от структурите с право на достъп при администратора. Извършването на периодична проверка се документира чрез съставяне на протокол *(Приложение № 16)*, в който се посочват мотивите, по които е взето решение за продължаване на съхранението на документи, съдържащи лични данни. Протоколите се съхраняват в служба „Архив".

5.Личните данни се унищожават, съгласно принципа за гарантиране подходящо ниво на сигурност, включително при съобразяване на мерки на защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане („цялостност и поверителност").

X. Трансфер на данни

1. Приема се, че всеки трансфер на данни от ЕС към страни извън ЕС са незаконни, освен когато се прилагат съответните гаранции или изключения за осигуряване на подходящо "ниво на защита на основните права на субектите на данни".

2. Решение за адекватност.

Европейската комисия може да оцени трети страни, територия и/или специфични сектори в трети страни, за да прецени дали има подходящо ниво на защита на правата и свободите на физическите лица. В тези случаи не се изисква разрешение.

Държавите, които са членки на Европейското икономическо пространство (ЕИП), но не и на ЕС, се приемат като отговарящи на условията за решение за адекватност.

Чл. 45 пар. 8 от ОРЗД - Комисията публикува в Официален вестник на Европейския съюз и на своя уебсайт списък на трети държави, територии и конкретни сектори в трета държава и международни организации, за които е решила, че осигуряват или че вече не осигуряват адекватно ниво на защита.

3. Изключения

При липса на решение за адекватност прехвърляне на лични данни в трета страна или международна организация се извършва при едно от следните условия:

- субектът на данните изрично се е съгласил с предложеното

прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;

- предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
- предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
- предаването е необходимо поради важни причини от обществен интерес;
- предаването е необходимо за установяването, упражняването или защитата на правни претенции;
- предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
- предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

XI. Регистър на обработванията на данни (инвентаризация на данните)

1. ПРБ поддържа Регистър на дейностите по обработване на лични данни.

2.При инвентаризацията на данните в ПРБ и в работния поток от данни се установяват:

- работните процеси, които използват лични данни;
- източниците на лични данни;
- броя на субектите на данни;
- описание на категориите лични данни и елементите на всяка категория;
- дейностите по обработване;
- целите на обработването, за което личните данни са предназначени;

- правното основание за обработването;
- получателите или категориите получатели на личните данни;
- основните системи и места за съхранение;
- всички лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и заличаване.

3. ПРБ е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. ПРБ оценява нивото на риска за лицата, свързани с обработването на личните им данни. Когато е задължително се извършват оценки на въздействието върху защитата на данните във връзка с обработването на лични данни от Администратора и във връзка с обработването, предприето от други организации от името на Администратора. *(Процедура за оценка на въздействието върху защитата на данните - Приложение № 10).*

4. Администраторът управлява всички рискове, идентифицирани от оценката на въздействието, с цел да се намали вероятността от несъответствие с правилата, заложени при изготвяне на оценката.

Когато вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване върху защитата на личните данни. Една обща оценка на въздействието може да разглежда набор от подобни операции по обработване, които представляват подобни високи рискове.

5. Когато в резултат на Оценката на въздействието е ясно, че Администраторът ще започне да обработва лични данни, които поради висок риск биха могли да причинят вреди на субектите на данни, решението дали обработването да продължи или не, трябва да бъде предадено за преглед от страна на Длъжностното лице за защита на данните, което да даде на ръководството писмено становище.

6. Ако ДЛЗД има сериозни опасения или относно потенциалната вреда или опасност, или относно количеството на съответните данни, то следва да отнесе въпроса пред надзорния орган.

Приложения: съгласно текста.

РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Задължението да се поддържа регистър на дейностите по обработване на лични данни произтича от обстоятелството, че ПРБ е администратор на лични данни. Поддържането на такъв регистър се възприема като:

- важна част от механизмите за отчетност и
- средство за извършване на анализ за евентуални усложнения, които може да породи обработването на данни.

ПРБ обработва лични данни за целите по чл. 42, ал. 1 от ЗЗЛД, както и за други цели (различни от тези по чл. 42, ал. 1 ЗЗЛД). Основанието за поддържане на регистър на дейностите по обработване произтича съответно от нормата на чл. 62, ал. 1 от ЗЗЛД и нормата на чл. 30, т. 1 от ОРЗД.

Регистърът се води в писмена форма и трябва да съдържа:

- Името и координатите за връзка на администратора и на длъжностното лице по защита на данните;
- Целите на обработването (например, управление на човешките ресурси, постигане на финансово-счетоводна отчетност, сключване и изпълнение на договори и др.);
- Описание на категориите субекти на данни и на категориите лични данни (посочва се качеството на субекта, в което участва в процеса – страна, свидетел, вещо лице и др. Обработваните лични данни за всяка категория субекти се описват общо, например данни за физическата идентичност на субектите – имена, ЕГН, адрес и т.н.);
- Категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- Когато е приложими, предаването на лични данни на трета държава или международна организация;
- Когато е възможно, предвидените срокове за изтриване на различните категории данни;
- Когато е възможно, общо описание на техническите и организационни мерки за сигурност.
- Съществена разлика в изискванията, определени в чл. 62, ал. 1 ЗЗЛД спрямо изискванията по чл. 30, пар. 1 от ОРЗД е изискването по ЗЗЛД в регистъра да се съдържа информация дали се извършва профилиране, когато това е приложимо. Няма пречка двата регистъра да се обединят и да се води единен регистър.

Няма задължение регистъра на дейностите по обработване на лични данни да се публикува.

Регистърът на дейностите по обработване на лични данни в ПРБ се поддържа от длъжностното лице по защита на данните и се публикува на вътрешно-ведомствената страница на ПРБ. Предложения за промени могат да се отправят към длъжностното лице по защита на данните от административните ръководители на прокуратури и ръководителите на почивни и учебни бази.

В структурите с право на достъп до лични данни при администратора-ПРБ се поддържа актуален списък на обработваните категории лични данни и въведените технически и организационни мерки на защита.

***Примерен образец на регистър на дейностите*:**

Описание на обработването	**Цели на извършеното обработване**	**Основание за обработване**	**Категории на личните данни**	**Чувствителни данни**	**Източник на данните**	**Категории субекти на данните**	**Получатели на данните**	**Трансфери извън ЕС**	**Оценка на риска и на въздействието**	**Мерки за сигурност**

ДЕКЛАРАЦИЯ

Долуподписаният/ата ……..,

ЕГН……., Л.К. № ……., издадена на ..... г.

от МВР гр. …….

в качеството си на …….

(длъжност/позиция)

в „……“,

ДЕКЛАРИРАМ:

1. Запознат/а съм с:

– нормативната уредба в областта на защитата на личните данни;

– политиката и ръководствата за защита на личните данни в ……;

– опасностите за личните данни, обработвани от администратора.

2. Поемам задължения за:

– несподеляне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

– неразгласяване на лични данни, до които съм получил/а достъп при и по повод изпълнение на задълженията си, ако това не е предвидено изрично в закон или не застрашава живота и здравето на физическото лице;

Дата:.....

ДЕКЛАРАТОР:……..

(подпис и фамилия)

гр./с/ …….

ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА ПРОЦЕСИТЕ ПРИ РАБОТА С КОНТРАГЕНТИ

I. Предназначение на процедурата

Тази процедура регламентира взаимоотношенията между Прокуратурата на Република България и всички външни контрагенти (подизпълнители, доставчици), във връзка с които съществува или може да се осъществи достъп до лични данни на субектите.
Това включва и контрагенти, които обработват лични данни от името на администратора, за достигане на определена от него цел. Тези лица се явяват в ролята на „обработващ лични данни“ по смисъла на ОРЗД.

II. Нормативна уредба

- Член 4, точка 8 и член 28 от Общия регламент за защита на данните (ОРЗД)

III. Задължения и роли

Ръководителите на структурните звена с право на достъп до лични данни при администратора-ПРБ са длъжни при възлагането на дейности, свързани с обработването на лични данни, да предприемат мерки, които да гарантират спазването на нормативните изисквания, както и да извършват одити или проверки на обработващите лични данни.

IV. Ход на процедурата

1. Ръководителите на структурните звена с право на достъп до лични данни при администратора-ПРБ избират само доставчици, които могат да осигурят техническа, физическа и организационна сигурност и които отговарят на поставените изисквания по отношение на всички лични данни, които ще обработват.
Сключването на договори, свързани с обработване на лични данни, се извършва само след съответното включване на предварително одобрени

клаузи/споразумения, предвидени за администратори или обработващи лични данни *(Приложение № 14 и Приложение № 15)*.

2. Доставчици от страни извън ЕС могат да бъдат избрани само при положение, че е изпълнено едно от следните специфични условия, изисквани в допълнение към останалите условия, посочени в тази процедура:

- ако доставчикът или държавата, в която пребивава или е установен, са били идентифицирани като осигуряващи адекватно ниво на защита на личните данни в решение за адекватност от страна на Европейската комисия,

или

- когато споразумението с доставчика е одобрено от надзорния орган.

3. Преди да бъде ангажиран външен контрагент по договор,

- основната причина, за сключването на който е дейност по обработване на лични данни, или
- с който ще бъдат обработвани лични данни извън минимално необходимите за идентифициране на страните и техните служители,

се извършва оценка на риска и в зависимост от нея, ако е необходимо - и въздействието върху защитата на данни (ОВЗД).

4. Ръководител на структурно звено с право на достъп до лични данни при администратора-ПРБ може (например, поради завишени изисквания по отношение защитата на чувствителни лични данни) да предприема действия по извършване на одит на системите за сигурност на доставчика съгласно изискванията на одобрени кодекси за поведение, фирмени правила или утвърдени стандарти за сигурност (например, ISO 27001 или съответни).

5. Прокуратурата сключва писмено споразумение с подизпълнителя за предоставяне на възложената услуга и изисква от контрагента да осигури подходящи мерки за сигурност на личните данни, които ще обработва. За целта в споразумението се предвиждат съответни гаранции, като например:

- Забрана доставчикът да използва от своя страна подизпълнители за обработването на личните данни без изрично писмено разрешение от съответния ръководител на структурно звено с право на достъп до лични данни при администратора-ПРБ. Когато ръководител разреши на доставчик да превъзложи обработването на лични данни на подизпълнител, доставчикът от първо ниво трябва да забрани на подизпълнителя от второ ниво (и по-нататък по веригата) да превъзлага дейността по обработване на данни на подизпълнители без писменото разрешение на съответния ръководител;

- 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 подизпълнител (доставчик). При прекратяването на договор с подизпълнител на второ и следващо ниво, съответните лични данни трябва да бъдат унищожени или върнати на ръководителя на структурното звено с право на достъп до лични данни при администратора-ПРБ по веригата от подизпълнители;
- Право на администратора/ръководителя на структурното звено с право на достъп до лични данни при администратора-ПРБ да извършва редовни проверки на системите за сигурност на доставчика през периода, в който той има достъп до личните данни.

V. Примерни образци

Договор за обработване на данни между администратор на лични данни и обработващ лични данни *(Приложение № 17).*

Клаузи между самостоятелни администратори

Примерни клаузи за поверително третиране на личните данни към договори между администратори – *(Приложение № 14).*

Примерни клаузи за поверително третиране към договор с обработващ – *(Приложение № 15).*

ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА ЗАЯВЛЕНИЯТА (ИСКАНИЯТА) ОТ СУБЕКТИТЕ

I. Предназначение на процедурата

Всички лични данни, обработвани от Прокуратурата на Република България, попадат в обхвата на тази процедура. Субектът на данни, може при упражняване на своите права, да отправи към Главния прокурор или определените от него лица (заместник на главен прокурор и административните ръководители на прокуратури) следните заявления/искания:

- Заявление/Искане за достъп (член 15 от ОРЗД);
- Заявление/Искане за коригиране (член 16 от ОРЗД);
- Заявление/Искане за изтриване („право да бъдеш забравен“) (член 17 от ОРЗД);
- Заявление/Искане за ограничаване на обработването (член 18 от ОРЗД);
- Възражение срещу обработване (член 21 от ОРЗД);

II. Нормативна уредба

- Членове 12, 15, 16, 17, 18, 20 и 21 от Общия регламент за защита на данните (ОРЗД)
- Членове 37а, 37б, 37в и 38 от Закона за защита на личните данни (ЗЗЛД)

III. Задължения и роли

Ръководителите на структурни звена с право на достъп до лични данни при администратора-ПРБ отговарят за прилагането и ефективното изпълнение на тази процедура и за уведомяване на собственика на информацията за исканията на субектите на данни.

Длъжностното лице по защита на данните оказва, при необходимост, съдействие при разглеждането на постъпили в ПРБ искания от субекти на данни.

IV. Ход на процедурата

Начините за подаването на искания до Администратора са описани в Процедура за начините на комуникация при жалби и искания от субекта на данни *(Приложение № 13)*.

1. Заявление за упражняване на правата на субектите на данни

Заявлението може да бъде подадено по следните начини:

- чрез писмено заявление до администратора на лични данни или по друг определен от администратора начин;
- по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация;

2. Отправяне на заявление/искане от субекта на данните

Исканията се правят, като се използва Образец на форма за заявление (искане) от субект на данните *(Приложение № 18)*. При отправянето на искане се спазват следните правила:

- Субектът на данни указва конкретния вид искане, съдържащ се в образеца на формата, предоставена от Администратора;
- Субектът на данните може да поиска информация относно всички негови лични данни, съхранявани от Прокуратурата на Република България без да указва конкретен вид;
- Субектът на данните предоставя на Администратора/ръководителя на структура с право на достъп до лични данни при администратора-ПРБ данни за самоличността си, които да го идентифицират сигурно и еднозначно (данни от лични документи, електронен подпис и т.н).
- Администраторът/ ръководителят на структура с право на достъп до лични данни при администратора-ПРБ задължително проверява идентификационните данни, за да се увери, че искането е подадено от субекта, който данните идентифицират;
- Администраторът/ ръководителят на структура с право на достъп до лични данни при администратора-ПРБ документира датата на получаване на искането;

- След като искането бъде получено, то незабавно се препраща до определените от главния прокурор лица, които задвижват процеса по обработка на искането и изпращането на отговор на субекта на данните.

3. Обработка на искането

Обработката на искането се извършва по следния начин:

- Ръководителите на структурни звена с право на достъп до лични данни при администратора-ПРБ и длъжностното лице по защита на данните поддържат дневник на исканията от субекти на данните;
- В дневника на исканията от субекти на данните се вписват датата, идентифициращата субектите информация и всички други важни за разглеждане на искането данни;
- Идентифицирането (търсенето) на личните данни се извършва във всички хранилища на данни и всички съответни системи за архивиране, включително всички архивирани файлове (автоматични или ръчни архиви) и всички папки на електронната поща и техните архиви;
- Когато искането е за достъп до информация, при предаването на копие от информацията се извършва, при необходимост, обработване на данните, с цел отстраняване на евентуална идентификационна информация за трети лица;
- Администраторът предоставя исканата информация и отговаря на исканията на субекта на данните в рамките най-късно на един месец от датата на получаване на искането за достъп;
- В дневника на исканията се вписват данни за подадения към субекта отговор на искането за достъп.

4. Допълнителна информация, изпращана при искане за достъп

В случай на искане за получаване на достъп до данни, освен осигуряване на достъп до данните (например, чрез предоставяне на тяхно копие), на субекта на данните се предоставя и следната информация:

- целите на обработването;
- съответните категории лични данни;
- получателите или категориите получатели на личните данни (ако има такива);

- информация относно намерението на Администратора да предаде данните на трета държава или на международна организация, както и наличието на гаранции за защита на данните;
- срока, за който Администраторът ще съхранява личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;
- правата 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;
- правото на жалба до надзорен орган;
- когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, Администраторът може:

- да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия;
- да откаже да предприеме действия по искането.

5. Действия при искания за коригиране, изтриване или ограничаване и при възражения срещу обработването

При искане на субекта на данни за коригиране, изтриване, ограничаване или при възражение по отношение на обработваните лични данни се извършва преценка на 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. Едва при положителна оценка исканията по упражняване на тези права се удовлетворяват.

След постъпването на съответното искане и установяване на неговата основателност:

- Администраторът/ръководителят на структурно звено с право на достъп до лични данни при администратора-ПРБ премахва личните данни от системите и прекратява операциите по обработката им, без ненужно забавяне, ако искането за изтриване е подадено от субекта на данните;

- Администраторът/ръководителят на структурно звено с право на достъп до лични данни при администратора-ПРБ съобщава за всяко извършено коригиране, изтриване или ограничаване на обработването на всеки получател, на когото личните данни са били предоставени – *Приложение № 19, Приложение № 20 и Приложение № 21;*
- Администраторът/ръководителят на структурно звено с право на достъп до лични данни при администратора-ПРБ информира субекта на данните относно тези получатели, ако субектът на данните поиска това, и документира това съобщение;
- Администраторът/ръководителят на структурно звено с право на достъп до лични данни при администратора-ПРБ взема подходящи мерки, без ненужно забавяне, в случай че:
  - субектът на данни е подал искане, с което възразява срещу обработването на личните данни изцяло или частично;
  - отпаднало е основанието за обработка по законово задължение;
  - данните са били незаконно обработвани.

V. Примерни образци

Образец на форма за Заявление (искане) от субект на данните *(Приложение № 18) и образци на уведомления (Приложения №№ 13, 19,20 и 21).*

ПРОЦЕДУРА ПО УВЕДОМЯВАНЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТА НА ЛИЧНИТЕ ДАННИ

I. Предназначение на процедурата

Тази процедура се прилага в случай на нарушение на сигурността на личните данни съгласно член 33 от ОРЗД – „Уведомяване на надзорния орган за нарушение на сигурността на личните данни“, и член 34 от ОРЗД – „Съобщаване на субекта на данните за нарушение на сигурността на личните данни“.

При изпълнението на процедурата следва да се има предвид, че ОРЗД прави разлика между администратор на лични данни и обработващ лични данни. Съгласно регламента, не всички организации, участващи в обработката на лични данни, носят една и съща степен на отговорност.

II. Нормативна уредба

- Член 33 и член 34 от Общия регламент за защита на данните (ОРЗД)
- Съображение 85 - 87 от Общия регламент за защита на данните (ОРЗД)

III. Задължения и роли

Настоящата процедура се прилага в случай на нарушение на сигурността на личните данни (виж Политика за провеждане на обучение *(Приложение № 6)*.

За всяко нарушение на сигурността на личните данни се докладва на ръководителя на структурното звено с право на достъп при администратора-ПРБ, респ. на длъжностното лице по защита на данните.

В случаите, когато нарушението на личните данни е свързано с информационната и комуникационната инфраструктура, задължително се уведомява ръководителя на звеното по информационна сигурност/директора на дирекция "Информационно обслужване и технологии" в АГП.

1. Процедура по уведомяване на надзорния орган

1.1. Ръководителите на организационни единици, в която е възникнало нарушението, незабавно уведомяват ръководителите на структурните звена с право на достъп при администратора-ПРБ, респективно длъжностното лице по защита на данните за наличието на нарушение на сигурността на личните данни.

1.2. Ръководителя на структурното звено с право на достъп при администратора-ПРБ, респ. длъжностното лице по защита на данните, уведомява главния прокурор за необходимостта от задействане на тази процедура и предприемането на необходимите стъпки.

1.3. Администраторът прави преценка дали е необходимо да се уведоми надзорния орган за нарушението. Съгласно член 33, параграф 1 от ОРЗД, не е необходимо да се изпраща уведомление, ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица.

1.4. Администраторът извършва оценка на риска. Уведомяването за нарушение е задължително, освен ако липсва вероятност то да породи риск за правата и свободите на физическите лица. Примери за такива вреди са дискриминация, кражба на самоличност или измама с фалшива самоличност, финансова загуба и накърняване на репутацията.

1.5. Ако след оценката на риска установи, че съществува риск за правата и свободите на субектите на данни, Администраторът уведомява надзорния орган за нарушението на сигурността на личните данни без ненужно забавяне и не по-късно от 72 часа след като е узнал за него (*Приложение № 22*). В случай че уведомлението не е направено в рамките на 72 часа, Длъжностното лице по защита на данните уведомява надзорния орган при първа възможност, като към уведомлението в допълнение излага причините за забавянето.

Уведомлението до надзорния орган трябва да съдържа следната информация:

- Описание на естеството на нарушението на сигурността на личните данни;
- Категориите лични данни, засегнати от нарушението;
- Категориите и приблизителният брой на засегнатите субекти на данни;
- Приблизителното количество на засегнатите записи на лични данни;
- Имената и контактните данни на Длъжностното лице по защита на данните;
- Описание на последиците от нарушението на сигурността;
- Предприетите или предложените от администратора мерки за справяне с нарушението.

Когато и доколкото не е възможно цялата необходима информация да се подаде едновременно, тя се подава поетапно без по-нататъшно ненужно забавяне.

Администраторът записва информацията относно потвърждението от страна на надзорния орган за получаването на уведомлението.

2. Процедура по изпращане на съобщение до субекта на данните

Когато има вероятност нарушението на сигурността на личните данни да ***породи висок риск*** за правата и свободите на субекти на данните, Администраторът, без ненужно забавяне, съобщава на засегнатите субекти на данните за нарушението. (*Виж Съобщение за нарушение от администратора на лични данни до субекта на данни - Приложение № 23).*

2.1. Преди да бъдат изпратени съобщения до субектите на данни, ДЛЗД проверява дали не са налице някои от основанията за отпадане на това задължението, а именно:

- Администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
- Администраторът е взел след разкриване на нарушението мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
- В случай че уведомяването на субектите би довело до непропорционално големи усилия за Администратора. В такъв случай се прави публично съобщение на интернет страницата или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

2.2. Съобщението до субекта/субектите на данни съдържа същата информация, която се изпраща и до надзорния орган, а именно:

- Описание на естеството на нарушението на сигурността на личните данни;
- Категориите лични данни, засегнати от нарушението;
- Категориите и приблизителният брой на засегнатите субекти на данни;
- Приблизителното количество на засегнатите записи на лични данни;
- Имената и контактните данни на Длъжностното лице по защита на данните / Отговорника по защита на данните;
- Описание на последиците от нарушението на сигурността;
- Предприетите или предложените от администратора мерки за справяне с нарушението.

Горната информация трябва да е описана на ясен и достъпен език.

В срок до 14 дни Администраторът предприема последващи мерки, които да

гарантират, че няма вероятност да се материализира високият риск за правата и свободите на субектите на данни.

2.3. Ако нарушението засяга голям брой субекти на данни и записи на лични данни, Администраторът взема решение, основано на оценка на количеството усилия, необходими за уведомяване поотделно на всеки субект на данни и на това дали по този начин би била възпрепятствана способността на Администратора да изпрати навреме нужните съобщения. Когато тази оценка покаже, че съобщаването до голям брой субекти би довело до непропорционални усилия, то Администраторът прави публично съобщение или взема друга подобна мярка, с която да гарантира, че субектите на данни ще бъдат в еднаква степен ефективно информирани.

Ако Администраторът не е съобщил на субекта/субектите на данните за нарушението на сигурността на личните данни и надзорният орган счита, че има голяма вероятност нарушението да породи висок риск, Администраторът съобщава на субекта/субектите на данните за нарушението в срок до 14 дни;

2.4. Административните ръководители и ДЗЛД документират в Регистър на нарушенията *(Приложение № 24)* всички нарушения на сигурността на личните данни, като посочва отнасящите се до тях факти, последиците и предприетите мерки за смекчаване на тяхното въздействие.

IV. Примерни образци

Съобщение за нарушение от администратора на лични данни до субекта на данни *(Приложение № 23)* и Регистър на нарушенията *(Приложение № 24)*.

ПОЛИТИКА ЗА ПРОВЕЖДАНЕ НА ОБУЧЕНИЕ

I. Обхват

Тези политика се отнася до програмата за обучение с цел постигане на оптимално ниво на компетентност на работещите в Администрацията на Прокуратурата на Република България, обслужва необходимостта от съответствие с изискванията на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните) и Закона за защита на личните данни при дейността на администрацията.

Настоящата политика се отнася също така до запознаването на служителите с установените от ПРБ политики, правила и процедури по защита на личните данни, задълженията на всеки служител съгласно тях, както и други въпроси, свързани със защитата на личните данни и неприкосновеността на личния живот.

Тази политика се отнася до непрекъснатото поддържане на осведомеността на служителите чрез обучение по вече наличните или нововъзникнали изисквания относно защитата на личните данни, както и предприетите от ПРБ мерки за съответствие с тях.

II. Задължения и отговорности

В структурите с право на достъп до лични данни при администратора се разпределят задължения и отговорности по защитата на данните във връзка с политиките, правилата и процедурите за обработване на лични данни.

Служителите на ръководна длъжност предприемат необходимото, така че всички служители от администрацията, които имат текущи задължения, свързани с операции по обработване на лични данни, както и тези с постоянен/редовен достъп до лични данни, да извършват работата си в съответствие с изискванията за защита на личните данни.

Тези служители трябва да могат да доказват компетентност в разбирането си относно изискванията за съответствие с Регламента, и как те се прилагат по отношение на тяхната дейност в Администрацията на ПРБ.

Служителите на ръководна длъжност, както и длъжностното лице по защита на данните отговарят тези служители да актуализират своите познания и да

бъдат информирани за всички въпроси, свързани с личните данни съгласно кръга на техните професионални задължения.

Ръководителите на структурите с право на достъп при администратора насърчават мерки за обучение и повишаване на осведомеността.

Прекият ръководител на съответното звено или определено от него лице запознава новоназначените служители със значението на защитата на данните в изпълнението на преките им задължения, като те получават и конкретно обучение за обработване на лични данни, свързано с техните постоянни служебни и трудови задължения и отговорности, в съответствие с настоящата Политика (например, но не само, запознаване с изготвени от Администратора/ДЛЗД ръководства, разяснения и становища …).

Длъжностното лице по защита на данните и съдебните администратори/административни секретари са задължени да проверяват периодично дали служителите разбират как и защо се прилагат правилата и процедурите на ПРБ за обработването на личните данни. Това може да става чрез периодични анкети за установяване и повишаване на познанията на служителите относно защитата на личните данни, включването на темите за защита на личните данни при организиране на семинари на други теми, както и чрез други подходящи форми.

Всеки новоназначен служител, чиято длъжност изисква обработването на лични данни, освен че подписва декларация за неразгласяване на лични данни, до които е получил достъп при и по повод изпълнение на задълженията си, подлежи и на обучение и инструктаж при назначаване. Това първоначално обучение се специфицира съобразно съответната позиция, като се започне с общо обучение, прилагано спрямо всички служители на администрацията, което се допълва с разяснение (инструктаж) за специфичните за длъжността задължения и изисквания за защита на личните данни. Така служителите получават конкретно обучение за обработване на лични данни, свързано с техните постоянни трудови/служебни задължения и отговорности и в съответствие с правилата и процедурите на ПРБ.

При обучението се разяснява, че всички служители отговарят за спазването на ограниченията за достъп до личните данни и носят дисциплинарна отговорност за нарушаването на принципите за поверителност, цялостност и наличност на личните данни.

Служителите получават конкретно обучение по всички изисквания и процедури за защита на информацията, приложими към защитата на данните и обработването на данни в рамките на техните задължения, включително докладване на нарушения на лични данни.

Служителите получават обучение относно постъпилите за разглеждане искания и възражения от субекти на данните, свързани със защитата на личните данни и обработването на лични данни, съгласно правилата и процедурите на ПРБ.

Ежегодните обучения (Приложение № 26) се провеждат в съответствие с правилата относно обучението на служителите в Администрацията на ПРБ. Информация за всяко проведено обучение се съхранява в база данни, поддържана от отдел „Човешки ресурси“ в АГП.

РЪКОВОДСТВО
за общо обучение по защита на личните данни

Раздел I. Цел

Настоящото ръководство предоставя общ преглед на необходимите знания по защита на личните данни и насочва към по-подробни изисквания, в зависимост от естеството на заеманата длъжност. Базирано е на Общия регламент относно защитата на личните данни и Закона за защита на личните данни в частта му, която го доразвива.

Раздел II. Основания

1. Общият регламент за защита на данните (ОРЗД), който е директно приложим в законодателството на България и се допълва чрез Закона за защита на личните данните (ЗЗЛД) и други нормативни актове, установява рамка от права и задължения, предназначени да защитават личните данни. Наред с тях администраторът на лични данни е изградил система от политики, процедури и изисквания относно защитата на личните данни в организацията, които са задължителни за магистратите и служителите.

Принципите за защита на личните данни

2. Принципите за защита на личните данни са установени в законодателството и са следните:
   2.1. Личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин.
   2.2. Личните данни, събирани за конкретни, изрично указани и легитимни цели, не се обработват по-нататък по начин, несъвместим с тези цели.
   2.3. Личните данни следва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват **(„свеждане на данните до минимум“)**.
   2.4. Личните данни следва да са точни и при необходимост да бъдат поддържани в актуален вид **(„точност“).**

2.5. Личните данни следва да са съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни **(„ограничение на съхранението“)**.

2.6. Прилагат се подходящи технически или организационни мерки срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане **(„цялостност и поверителност“)**.

Права на субектите на данни

3. ОРЗД задава определени права на субектите на данни, свързани с техните лични данни, които са:
   - право на достъп;
   - право на коригиране;
   - право на изтриване (при определени обстоятелства) – правото „да бъдеш забравен“;
   - правото за ограничаване на обработването;
   - право на преносимост (при определени обстоятелства);
   - правото за възражение;
   - правото да се изисква човешка намеса с оглед на автоматизирани процеси, включително профилиране.
4. Правото на субектите на лични данни по закон следва да се реализират в определен срок от един месец. Поради това от съществено значение е своевременното разглеждане от административните ръководители на прокуратури и, при необходимост, предоставянето на исканията от субекти на лични данни на Длъжностното лице по защита на данните във възможно най-кратък срок след тяхното получаване.

Лични данни. Категории.

5. Дефиниране на „лични данни“ и „специални категории лични данни“ (чувствителни данни), съгласно ОРЗД:
   5.1. „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да

бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

5.2.„специални категории лични данни“ са лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице;

Основания за обработване

6. Всяко обработване на лични данни следва да почива на поне едно законово основание, съгласно ОРЗД. Възможните основания са (чл. 6 от ОРЗД): договор, законово задължение, жизненоважни интерес, обществен интерес, легитимен интерес и съгласие. Данните за специалните категории изискват по-специално законово основание (чл. 9 от ОРЗД). Тази законова основа се посочва в Регистър на дейностите по обработването. Служител, който не е сигурен какво правно основание се отнася до личните данни, които възнамерява да обработва, трябва да потърси съвет от Длъжностното лице по защита на личните данни. ПРБ обработва лични данни най-вече на основание на закона, т.е. извършването на определената услуга е регламентирано в закон или в подзаконов акт. Това налага познаване на нормативната уредба в съответната сфера, в която работи служителя, защото правното основание за обработване на личните данни често е и правната разпоредба, където е предвидено определено право за гражданите.
7. Администраторите на лични данни обикновено обработват лична информация за своите служители, договорни партньори и др., определени като субекти на данни в законодателството за защита на данните. Тези данни трябва да се обработват само в съответствие със законодателството за защита на данните и с вътрешните изисквания за това. В противен

случай има нарушение на законодателството за защита на данните и се носи отговорност за последиците от такова нарушение.

8. Ръководителите на структурите с право на достъп до лични данни ПРБ отговарят за спазването на законодателството за защита на данните. Всички служители трябва да са преминали първоначално общо и първоначално специализирано обучение, преди да имат достъп до лични данни, обработвани от ПРБ. Обръща се особено внимание и се изисква познаване и на правилата и инструкциите за работа със специализираните информационни системи в институцията, наред с познаването на всички вътрешни правила, действащи в нея.
9. Отговорност на всички служители в организацията на Администратора е да се гарантира сигурността на личните данни. Личните данни не трябва да се разкриват на никое неупълномощено лице под каквато и да е форма, случайно или по друг начин.
10. Всяко нарушение или неспазване на правните норми, правилата и процедурите, особено всяко преднамерено разкриване на лични данни на неупълномощена страна, може да доведе до дисциплинарни или други подходящи действия.

Изрични ограничения в практиката.

Действия при нарушение на поверителността.

11. Важно е да се знае от всички служители, които събират лични данни пряко от субектите на данни, че копирането на документ за самоличност, свидетелство за управление на моторно превозно средство или документ за пребиваване е допустимо само ако е предвидено със закон или подзаконов нормативен акт. Например е допустимо копирането и съхранението на свидетелство за управление на моторно превозно средство при наемане за длъжността „шофьор“ за доказване на съответната квалификация или правоспособност на шофьора и за целите на съответното трудово правоотношение. Съответно при обичайното кандидатстване и постъпване на работа личната карта не се копира, а се събират данните от нея.
12. Всеки неоторизиран достъп до или разкриване на лични данни или други нарушения на сигурността на данните трябва да бъде докладван от служителите, които ги установят, на ръководството или ДЛЗД, съгласно

Политиката за защита на личните данни в АГП веднага след установяването им или при наличието на основателно подозрение за настъпило нарушение. Редът за действие по-нататък е развит в Процедура по уведомяване за нарушение на сигурността на личните данни.

13. Нарушаването на поверителността на личните данни е и нарушение на законодателството за защита на данните и може да доведе до административно-наказателна и гражданска отговорност на Администратора. Следователно всички, имащи достъп до лични данни в организацията трябва да се придържат към разпоредбите на законодателството, индивидуалните си задължения по съответния договор и/или длъжностна характеристика, към правилата за защита на личните данни и допълнителните изисквания, приети от Администратора.
14. Личните данни се съхраняват само за времето, необходимо за извършване на обработването, за което са събрани. Това важи както за съхранявани на електронен носител, така и за тези на хартия. Това се разпростира също така и върху резервните копия и копията, направени на преносими носители.

Технически и организационни мерки

15. Регистърът на дейностите по обработването се използва, за да се отговори на изискванията за отчетност при съхранение на данни в законодателството за защита на данните.
16. Служителите, отговарящите за отделните организационни и оперативни дейности, които формират *целите* на обработваната информация, осигурят създаването и поддържането **на актуалността на информацията в регистъра.** Всяка година те извършват преглед на актуалността.
17. В организацията на Администратора се въвеждат подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с ОРЗД, като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица. Техническите и организационните мерки следва да допринесат за защита на данните на етапа на проектирането и по подразбиране.

18. Всеки трансфер на данни, включително използването на облачни услуги, извън ЕИП следва да бъде предварително съгласуван с ръководството и ДЛЗД с оглед изискването в ОРЗД за предприемането на определени мерки. Условията, при които личните данни могат да бъдат прехвърлени в страни извън Европейското икономическо пространство, са определени в ОРЗД. Те включват адекватност (решение на ЕК за адекватно ниво на защита), подходящи гаранции (например чрез инструмент със задължителен характер и с изпълнителна сила между публичните органи или структури), както и други.

ОБРАЗЕЦ НА ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ НА СУБЕКТА НА ДАННИТЕ

Аз, долуподписан/ият/та

.....

(име на субекта на данните, друга информация за идентификация),

с настоящото декларирам, че давам съгласие на администратора на лични данни Прокуратура на Република България, 1061 София, бул. „Витоша“ № 2

.....

(име на администратора, данни за идентификация)

да обработва моите лични данни за целите на:

.....

(*изрично уточнете целите, които се преследват с обработването на тези лични данни, както и точно описание на данните*).

Съзнавам, че мога да оттегля моето съгласие по всяко време чрез Образец на форма за оттегляне на съгласие от субекта на данните *(Приложение № 12)*.

Съзнавам, че оттеглянето на съгласието ми по-късно няма да засегне законосъобразността на обработването, основано на дадено сега съгласие.

Съзнавам, че в качеството ми на субект на данни и във връзка с даденото от мен съгласие имам правата по представеното ми от администратора Уведомление за поверително третиране на личните данни (*Декларация за поверителност- Приложение № 9*).

Подпис на субекта на данните:

Дата:

Получено от:.....на.....

ПРОЦЕДУРА ЗА ПРОЗРАЧНОСТ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

I. Предназначение на процедурата

Настоящата процедура обхваща всички дейности по събиране и обработване на лични данни от Прокуратурата на Република България.

II. Нормативна уредба

Член 12, 13 и 14 от Общия регламент относно защитата на данните (ОРЗД)

Чл. 25а, чл. 25д, чл. 25и от Закона за защита на личните данни (ЗЗЛД)

III. Задължения и отговорни лица

Изискването за прозрачност съществува напълно независимо от изискването за администратора да гарантира, че съществува подходящо правно основание за обработването на данни.

Ръководителите на структурите с право на достъп до лични данни при администратора-ПРБ и служителите в Администрацията на ПРБ са отговорни за прилагането и изпълнението на задълженията по тази процедура.

Всички служители на ПРБ, които по силата на своите трудови/служебни задължения събират лични данни, трябва да спазват настоящата процедура.

IV. Ход на процедурата

1. Информационни съобщения за прозрачност към субекта на лични данни

ПРБ, съгласно изискванията на ОРЗД, предоставя на субектите на данни законово изискваната информация във вид на Уведомление за поверително третиране на личните данни *(Приложение № 9)* и Съобщение за условия за използване на бисквитки *(Приложение № 25)*.

Ръководителите на структурите с право на достъп до лични данни поставят тези съобщения на интернет страниците на съответните прокуратури.

На официалната интернет страница на Прокуратурата на РБ на адрес www.prb.bg се публикува в ясно обособена секция "Защита на личните данни“ Уведомление за поверително третиране на личните данни (Декларация за поверителност- *Приложение № 9*).

В бланковите документи и формуляри, които се използват при предоставянето на административни услуги, при кандидатстване за работа в ПРБ, както и в др. случаи, се поставя специален текст, който да насочва към секция на интернет портала на ПРБ, която съдържа „Уведомление за поверително третиране на личните данни“, което се отнася до съответните субекти:

„В качеството си на администратор на лични данни ПРБ обработва лични данни при стриктно спазване на разпоредбите на Регламент 2016/679 и Закона за защита на личните данни. Допълнителна информация как и защо ПРБ обработва лични данни, се съдържа в секцията „Защита на личните данни“ на нашия интернет сайт: https://prb.bg/bg/7554.

Възможно е също така предоставянето на субектите на данни на тази информация (уведомление за поверително третиране на личните данни) да става физически на самите гишета под формата на информационни табели в по-съкратен или по-разширен формат.

На видно място в зоните, над които се осъществява видеонаблюдение се поставят съобщения, които уведомяват субектите на данни:

„В сградата се осъществява постоянно видеонаблюдение за целите на охраната“

На интернет страницата на ПРБ се поставя уведомление за използваните от сайта бисквитки (cookies), по начин, който да гарантира прочитането им от потребителите, както и даване на изрично съгласие за използването им. Описанието им и начина на действие са в отделен документ Съобщение за условия за използване на бисквитки *(Приложение № 25)*.

1.1 При събиране на лични данни от субекта на данни се предоставя следната информация:

- данните, които идентифицират Администратора и координатите за връзка с него.
- данните за контакт с Длъжностното лице по защита на данните.

- данните, които идентифицират представителя на администратора;
- целите на обработването, за което личните данни са предназначени;
- правното основание за обработването на личните данни;
- когато е уместно, легитимните интереси на ПРБ, които осигуряват правната основа за обработката;
- категориите лични данни, които се обработват;
- получателите или категориите получатели на личните данни (ако има такива);
- информация относно намерението на Администратора да предаде данните на трета държава или на международна организация, както и наличието на гаранции за защита на данните;
- срока, за който ще се съхраняват личните данни от Администратора, а ако това е невъзможно, критериите, използвани за определяне на този срок;
- указание към субекта на лични данни за правата му да изиска от Администратора достъп до данните, 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;
- когато правното основание за обработването е съгласие, Администраторът уведомява субекта на данни за съществуването на право на оттегляне на съгласието по всяко време, както и за законосъобразността на обработването до момента на оттегляне;
- правото на жалба до надзорен орган;
- наличието на автоматизирано вземане на решения, включително профилиране, както и предвидените последствия от това обработване за субекта на данните.
- когато правното основание не е съгласие на субекта, а е задължително или договорно изискване, или изискване, необходимо за сключването на договор, Администраторът уведомява субекта на данни за това, а също и дали е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени.

1.2 Когато лични данни са получени от източник, РАЗЛИЧЕН от субекта на данните ПРБ предоставя следната информация:

- данните, които идентифицират ПРБ и координатите за връзка;
- данните за контакт с Длъжностното лице по защита на данните;
- целите на обработването;
- правното основание за обработването;
- категориите лични данни, които се обработват;
- потенциалните получатели / категориите получатели на личните данни;
- намерението на ПРБ да извърши предаване на данните на трета държава извън ЕС или на международна организация, съответните гаранции за защита на данните и средствата за получаване на копие от тях или на информация къде са налични;
- указание към субекта на лични данни за правата му да изиска достъп до данните, коригиране или изтриване на неговите лични данни, както и правата му на ограничаване на обработването, на възражение срещу обработването и на преносимост на данните;
- когато правното основание за обработването е съгласие, Администраторът уведомява субекта на данни за съществуването на право на оттегляне на съгласието по всяко време, както и за законосъобразността на обработването до момента на оттегляне;
- правото на жалба до надзорен орган;
- източника на личните данни и дали данните са от публично достъпен източник;
- наличието на автоматизирано вземане на решения, включително профилиране, както и предвидените последствия от това обработване за субекта на данните;
- срокът, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок.

2. **Срокове, изключения и начин на предоставяне на информацията**

При предоставянето на информацията, Администраторът спазва следните изисквания на ОРЗД:

- При събирането на лични данни от субекта на данни Администраторът предоставя на субекта посочената информация в момента на получаване на информацията;

- При събирането на лични данни от източник, РАЗЛИЧЕН от субекта на данните, Администраторът предоставя на субекта посочената информация в срок до един месец от получаване на личните данни в съответствие със специфичните обстоятелства на обработката;
- В случаите, когато данните се използват за комуникация със субекта на данни, Администраторът съобщава информацията най-късно при осъществяване на първия контакт с него;
- В случаите, когато личните данни се разкриват на друг получател, Администраторът съобщава информацията най-късно при разкриването на личните данни за първи път;
- Администраторът НЕ предоставя тази информация, ако субектът на данните вече разполага с нея;
- Администраторът НЕ предоставя тази информация, в случай, че предоставянето се окаже невъзможно или би довело до прекомерно усилие;
- Администраторът няма задължение да предостави тази информация, ако личните данни трябва да останат поверителни при спазване на задължение за професионална тайна, регламентирано от националното законодателство, включително законово задължение за тайна;
- Администраторът предоставя на субекта на данните всяка допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване;
- цялата информация, предоставена на субекта на данни, е в лесно достъпен формат, като се използва ясен език.

V. Особени случаи на обработване

В чл. 25и от ЗЗЛД към работодателите или органите по назначаване е поставено изискване за приемане на правила и процедури при:

- използване на система за докладване на нарушения;
- ограничения при използване на вътрешнофирмени ресурси;
- въвеждане на системи за контрол на достъпа, работното време и трудовата дисциплина.

Съгласно чл. 25и, ал. 3 от ЗЗЛД работодателят е длъжен да уведоми

работниците и служителите за правилата и процедурите, които е въвел.

Това изискване се изпълнява от администратора-ПРБ чрез публикуване на вътрешноведомствените актове на ведомствената интернет-страница на ПРБ.

VI. Примерни образци

- Уведомление за поверително третиране на личните данни (Декларация за поверителност) *(Приложение № 9)*
- Съобщение за условия за използване на бисквитки *(Приложение № 25)*
- Образец на форма за заявление/искане от субект на данните *(Приложение № 18)*

ОБРАЗЕЦ НА УВЕДОМЛЕНИЕ ЗА ПОВЕРИТЕЛНО ТРЕТИРАНЕ НА ЛИЧНИТЕ ДАННИ (ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ)

Уведомление за поверително третиране на личните данни

Прокуратурата на Република България (ПРБ) в рамките на своите конституционни правомощия следи за спазване на законността, като ръководи разследването и упражнява надзор за законосъобразното му провеждане; може да извършва разследване; привлича към отговорност лицата, които са извършили престъпления, и поддържа обвинението по наказателни дела от общ характер; упражнява надзор при изпълнение на наказателните и други принудителни мерки; предприема действия за отмяна на незаконосъобразни актове; в предвидените със закон случаи участва в граждански и административни дела.

Дейността на администрацията на ПРБ се осъществява според правната рамка на Правилника за администрацията на Прокуратурата на Република България.

За контакт с Прокуратурата на Република България:

София 1061, бул. „Витоша" № 2

Електронна поща: prbcont@prb.bg

Интернет страница: www.prb.bg

Като администратор на лични данни Прокуратурата на Република България осъществява дейността си в съответствие с Общия регламент относно защитата на данните (ОРЗД), Закона за защита на личните данни и другите европейски и български нормативни актове в областта на защитата на личните данни. ПРБ спазва следните принципи при обработването на лични данни:

- законосъобразност, добросъвестност и прозрачност;
- ограничение на целите на обработване;
- съотносимост с целите на обработването и свеждане до минимум на събираните данни;
- точност и актуалност на данните;
- ограничение на съхранението с оглед постигане на целите;
- цялостност и поверителност на обработването и гарантиране на подходящо ниво на сигурност на личните данни.

Общият регламент относно защитата на данните, както и Закона за защита на личните данни изискват от администраторите на лични данни да предоставят определена информация на лицата относно начина на използване (обработване) на техните лични данни.

Правни основания за обработване на лични данни от администрацията на Прокуратурата на Република България

Администрацията на прокуратурата осъществява своята дейност на основание Правилника за дейността на администрацията на Прокуратурата на Република България в интерес на обществото и съдебната власт и в съответствие с Конституцията, Закона за съдебната власт и с други нормативни актове. Администрацията в различните направления на дейността си обработва лични данни на различни правни основания по Общия регламент относно защитата на данните.

Най-често администрацията на ПРБ обработва лични данни в изпълнение на конкретно правно задължение, произтичащо от различни нормативни актове - ЗСВ, ПАПРБ, ЗМВР, ЗДСл, КТ, ЗДОИ, ЗЗЛД, ЗЗД, КСО, ЗСч, ЗДДФЛ, ЗНАФ, НРВПО и тогава правното основание е:

- чл. 6, параграф 1, б. „в“ от ОРЗД - спазването на законово задължение, което се прилага спрямо администратора;

Когато администрацията на ПРБ изисква и обработва данни за присъди, които се съдържат в свидетелствата за съдимост, то също е в изпълнение на конкретно законово задължение за спазване на изискванията за заемане на съответната длъжност.

За целите на сключване и изпълнение на договори администрацията на ПРБ се позовава на :

- чл. 6, параграф 1, б. „б“ от ОРЗД - изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

Когато обработва чувствителни данни, каквито са например данните за здравето, администрацията на ПРБ се съобразява с допълнителните изисквания на ОРЗД. Така администрацията на ПРБ обработва чувствителни данни на основание:

- чл. 9, параграф 2, б. „б“ и „з“ от ОРЗД - за целите на изпълнението на задълженията на администратора по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила, доколкото това е разрешено от българското законодателство, както и за целите на трудовата медицина.

Обработването на лични данни от видеонаблюдението се извършва с цел охрана на хора и имущество, както и за контрол на работното време.

По изключение е възможно да се осъществява конкретна дейност на обработване на основание чл. 6, параграф 1, б. „а“ от ОРЗД - субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели.

Права на субектите на данни при дейността на администрацията на ПРБ

Във връзка с извършваната от администрацията на ПРБ дейност и обработваните техни лични данни субектите на данни имат право на :

- Достъп до личните им данни;
- Коригиране или изтриване на личните им данни;
- Ограничаване на обработването им;
- Право на възражение срещу обработването на техните данни;
- Преносимост на данните (при определени предпоставки);
- Право да не бъдат обект на изцяло автоматизирано решение, включващо профилиране.

Правата се упражняват по заявление като се използва определената за това бланка и се подава по някой от посочените в настоящето уведомление канали за комуникация. Администрацията на ПРБ ще приеме искането и ако е не използвана предоставената форма, но при всички случаи, за да бъде разгледано, то трябва да отговоря на минималните законови изисквания – да е в писмена форма и да съдържа:

1. Име, адрес, единен граждански номер или личен номер на чужденец или друг аналогичен идентификатор, или други идентификационни данни на физическото лице, определени от администратора, във връзка с извършваната от него дейност;
2. Описание на искането;
3. Предпочитана форма за получаване на информация при упражняване на правата по чл. 15 – 22 от Регламент (ЕС) 2016/679;
4. Подпис, дата на подаване на заявлението и адрес за кореспонденция.
5. При подаването на заявление от упълномощено лице към заявлението се прилага и пълномощното.

Образец на искане за упражняване на правата на субектите на лични данни може да намерите тук.

По всички въпроси, свързани с обработването на лични данни при дейността на администрацията на Прокуратурата и с упражняването на правата им, субектите на данни могат да се обърнат към определеното от Прокуратурата на Република България длъжностно лице по защита на данните - bjankov@prb.bg.

Право на жалба до КЗЛД

Според Общия регламент относно защитата на данните субектите на данни имат право на жалба до надзорен орган във връзка с обработването на техните лични данни от администрацията на Прокуратурата. Надзорен орган в Република България върху дейността по защита на личните данни в ПРБ извън дейността й на орган на съдебна власт е Комисията за защита на личните данни, гр. София 1592, бул. „Проф. Цветан Лазаров" № 2, тел.: +359 2 915 3 518, kzld@government.bg, kzld@cpdp.bg, www.cpdp.bg

Колко време се съхраняват личните данни

Информацията се поддържа точна и актуална и не се съхранява за по-дълго от необходимото време. Сроковете на съхранение на личните данни са съобразени с определеното в нормативните актове и Номенклатурата на делата в ПРБ, която се поддържа в съответствие със Закона за Националния архивен фонд

1. ***Информация за кандидати за работа***

Цели на обработването и правни основания

Обработването на лични данни в процеса на набиране на нови служители е с цел да се прецени дали кандидатът е подходящ за длъжността, за която кандидатства, както и с цел осъществяване на контакт.

Правното основание, въз основа на което се обработват лични данни, е смесено:

- Съгласие на кандидата – по чл. 6, параграф 1, б. „а“ от ОРЗД – относно обработването на личните данни за целите на кандидатстването или конкурса, изразено чрез фактическите действия по подаване на документите и
- Обработването е необходимо за спазването на законово задължение по изискване на определени документи - чл. 6, параграф 1, б. „б“ от ОРЗД, а по отношение специалните категории лични данни се прилага чл. 9, параграф 2, б. б) от ОРЗД във връзка с трудовото законодателство на Република България.
- Когато администрацията на ПРБ изисква и обработва данни за присъди, които се съдържат в свидетелството за съдимост, това се прави също в изпълнение на конкретно законово задължение по изискванията за заемане на съответната длъжност.

Резултати от процедурите по подбор на персонала се публикуват на официалния сайт и на общодостъпно място.

Данни, които се обработват

Основните категории данни са:

- Лична информация – имена, дата на раждане, месторождение, българско гражданство, както и информация за контакт – адрес за кореспонденция, телефонен номер, ел. поща и др.
- Информация за образователна подготовка – образователна степен, допълнителна квалификация и др.
- Информация за професионален опит – предходни или настоящи организации, в които кандидатът е работил, упражняване на свободни професии и др.

Във връзка със специфични нормативни изисквания за конкурсите за встъпване в трудово правоотношение като съдебен служител е възможно обработване на специални категории данни

като данни за здравословното състояние и др., лични данни, свързани с присъди и нарушения, както и данни, свързани с политически неутралитет.

На кого се предоставят личните данни

Като правило тези лични данни не се предоставят на трети лица.

Автоматизирано вземане на решения и профилиране

Администрацията на Прокуратурата на Република България не използва личните данни, събрани в процеса на кандидатстване за работа, за автоматизирано вземане на решения посредством компютърни алгоритми, заменящи човешката преценка, включително чрез извършване на профилиране.

Срок, за който ще се съхраняват личните данни

За неизбраните кандидати предоставените лични данни се унищожават не по-късно от законовия срок, след приключване на конкурсната или друга процедура по избор на кандидати.

В случай че са представени оригинали или нотариално заверени копия на документи, които удостоверяват физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, те се връщат на субекта на данни, който не е одобрен за назначаване, в 6-месечен срок от окончателното приключване на процедурата. Вътрешни документи на органа от проведения конкурс или кандидатстване се съхраняват до 3 години.

2. ***Информация за настоящи и бивши служители***

Прокуратурата на Република България обработва лични данни на прокурори, следователи, съдебни служители, служители по ЗМВР, държавни служители, лица по трудово правоотношение и изпълнители по граждански договори.

Цели на обработването и правни основания

Основните цели на обработване на личните данни на настоящи и бивши магистрати и съдебни служители в Прокуратурата на Република България са :

- Да се осигури изплащане на съответните възнаграждения и обезщетения, да се осъществи задължителното обществено и здравно осигуряване и застраховане, да се осигурят здравословни и безопасни условия на труд;
- Да се подържа и актуализира съответното кадрово досие;
- Да се подготви и предостави информация до други публични органи;
- Да се издаде трудова или служебна книжка;
- Да се издаде служебна карта;
- Да се осъществява контакт със съответния служител;
- Да се осъществят обучителни мероприятия и да се осигури почивка на магистрати и съдебни служители на Прокуратурата на Република България, членовете на техните семейства и други придружаващи лица в учебните бази на ПРБ.

Правното основание, въз основа на което се обработват личните данни, е основно изпълнение на законово задължение (чл. 6, ал. 1, б. „в“ от ОРЗД), а именно:

- Данните във връзка със сключването на трудов договор като съдебен служител се обработват в изпълнение на Закона за съдебната власт, Кодекса на труда и Правилника за администрацията на Прокуратурата на Република България, а данните за встъпване в служебно правоотношение се обработват в изпълнение на ЗСВ, ЗЗЛЗВНП и ЗМВР.
- Данните относно здравето в хода на трудовото или служебното правоотношение се обработват в изпълнение на Кодекса на труда, ЗСВ, ЗМВР, Закона за здравето и съответни подзаконови нормативни актове.
- По отношение на специфичната информация, обработвана за магистратите, съдебните и държавните служители, ПРБ изпълнява задължения и по Закона за съдебната власт, Закона

за противодействие на корупцията и за отнемане на незаконно придобитото имущество, както и Правилника за администрацията на Прокуратурата на Република България по отношение на правилата за несъвместимост.

- За конкретни длъжности и конкретни случаи, възникнали в хода на трудовото или служебно правоотношение, се изпълняват и специални изисквания на изброените вече нормативни актове, както и на други относими такива.
- Когато личните данни се обработват във връзка с използване на учебните бази на ПРБ това става на основание заявено съгласие от съответните субекти чрез подаване на заявка за ползването им, както и на основание изискванията на Закона за туризма.
- Обработването на лични данни при ползването на ведомствени жилища се осъществява на основание съгласие, заявено чрез кандидатстване за такова жилище, както и при спазване разпоредбите на ЗДС, ППЗДС и издадените в изпълнение на закона Правила за отдаване под наем на недвижими имоти - частна държавна собственост, предоставени в управление на ВСС за жилищни нужди.

Данни, които се обработват

Основните категории данни, които се обработват, са:

1. Предоставените от субекта на данни и събрани в хода на кандидатстването му за съответната позиция, които се съхраняват в кадровото досие.

2. Данни, необходими за сключване на трудов договор или изготвяне на актове за назначение, а именно:

- Физическа идентичност – имена, ЕГН, адрес, данни от документа за самоличност, месторождение, телефон
- Социална идентичност - придобито образование, специалност, квалификация, правоспособност, които се изискват за длъжността, професионален опит, информация за ползван платен годишен отпуск
- Данни относно здравето – под формата на документ за медицински преглед, и декларация, че не сте поставени под запрещение
- Данни, свързани с присъди и нарушения – въз основа на законово задължение за конкретната длъжност
- Информация, изискуема във връзка с правилата за несъвместимост – информация, свързана със заемането на друга длъжност или извършване на търговска дейност, относно роднинска връзка или фактическо съжителство с лица, с които бихте се оказали в йерархическа връзка на ръководство и контрол, както и информация, свързана с ръководна или контролна длъжност в политически партии.
- Информация във връзка с имущество и интереси – информация за имотно състояние и доходи, както и информация за доходите на съпруг/съпруга, свързана с антикорупционното законодателство, а така също и при кандидатстване за ползване на ведомствено жилище.

3. Информация, събирана в хода на служебното или трудово правоотношение:

- Икономическа идентичност – осигурителен доход, размер на възнаграждение;
- Информация във връзка с имущество и интереси – ежегодна информация за имотно състояние, доходи, както и информация за доходите на съпруг/съпруга, свързана с антикорупционното законодателство; имотно състояние, участие и/или притежаване на дялове или ценни книжа в дружества;
- Информация, свързана със съществуване, изменение и прекратяване на трудовото или служебно правоотношение
- Данни относно здравето – информация от болнични листове, ТЕЛК и др.

- Социална идентичност – произход, среда, заемана длъжност в администрацията, образование, трудова дейност; данни относно отглеждани деца в случай на наложен запор на трудово/служебно възнаграждение.
- Данни за съществуващи задължения - в случай на наложен запор на трудово/ служебно възнаграждение.
- Данни за членовете на семействата при ползване на учебните бази и ведомствени жилища.

Източник на данните

По-голямата част от информацията, с която администрацията на ПРБ разполага, се предоставя от субектите на данни лично.

Част от документите, удостоверяващи обработвана информация, се приемат само с цел снемане на съответната информация. Администрацията на ПРБ не събира копия или оригинали на документи, в случай че няма нормативно основание за това.

На кого се предоставят личните данни

Като правило ПРБ не предоставя тези лични данни на трети лица, освен в случаи, в които това е определено в закона като посочените по долу.

Информация за служители на ПРБ се предоставя на трети лица, основно публични органи, във връзка с изискванията на законодателството в Република България. Получатели на информация могат да са: Главна инспекция по труда, НАП, НОИ, съдебни изпълнители, ВСС, Инспектората към ВСС, НИП, КПКОНПИ, АДФИ, Сметна палата, служба по трудова медицина и др.

Автоматизирано вземане на решения и профилиране

ПРБ не използва личните данните, събрани във връзка с качеството на служител в ПРБ, за автоматизирано вземане на решения посредством компютърни алгоритми, заменящи човешката преценка, включително чрез извършване на профилиране.

3. Информация за посетители на сайта на ПРБ

Интернет страницата на Прокуратурата на Република България е основно средство за информиране и комуникация с граждани. На сайта се публикуват често задавани въпроси, доклади и анализи, искания и становища по конституционни и тълкувателни дела, актове за обществени консултации, вътрешни и междуведомствени актове, справки по години за досъдебни производства, преписки по следствения и надзора за законност, новини и информация, касаеща гражданите, като тази за дела от обществен интерес и др. Така публикуваната информация не съдържа лични данни.

Наред с това административните услуги, които ПРБ предлага на гражданите, налагат обработването на лични данни. Определени услуги се предоставят на сайта чрез е-подпис.

Сигнали до прокуратурата могат да се подават и в електронен вид чрез попълване на електронна форма при събиране на необходимите данни от подателя с цел да се избегне третиране на сигнала като „анонимен" и оставянето му без разглеждане.

Обработвани данни и цели

В рамките на услугите, които са достъпни през интернет страницата, ПРБ обработва:

- Данни за идентификация – три имена, точен пощенски адрес, телефон с цел да се идентифицира подателя на сигнала, а също и че се предоставя информация на лицето, което я е поискало. По – голямата част от услугите са достъпни чрез използване на е-подпис.
- Допълнителни данни – информация, която субектите на данни доброволно предоставят с цел обработване на сигнал или получаване на поисканата информация по ЗДОИ.

- Данни, свързани с използването на интернет страницата – Прокуратурата, може да обработва данни, включително IP адреси на потребители във връзка с постигане адекватно ниво на информационна сигурност.

Сигурността на интернет страницата на ПРБ се гарантира от прилагането на адекватни технически и организационни мерки. Трансферът на данни между потребителя и сайта се осъществява посредством SSL протокол, който осигурява конфиденциалността и интегритета на данните.

(Вижте и Условията за използване на бисквитки)

4. Информация за лица, чиито данни се обработват за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления

Прокуратурата на Република България (ПРБ), в качеството ѝ на орган на съдебна власт, обработва лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания.

Във връзка с изпълнение на конституционните си правомощия Прокуратурата на Република България се явява администратор на лични данни по смисъла на Глава осма от Закона за защита на личните данни.

Цели на обработването и правни основания

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, както и изпълнението на наказанията (ЗСВ, НПК, АПК, ЗИНЗС).

Категории субекти на данни

Това са лицата по прокурорски преписки, участници в досъдебното и съдебното производство, лица, изтърпяващи наказание. Също така и лица, застрашени във връзка с наказателно производство, лица, охранявани при условията и по реда на НПК, лица, принудително довеждани до орган на съдебната власт по разпореждане на главния прокурор.

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 и защитата на застрашени лица.

Категориите получатели, пред които се разкриват личните данни

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

Права на субектите на лични данни по Глава осма от ЗЗЛД

При обработването на лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания субектът на данни има следните права:

- 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 обработваните категории лични данни и личните данни, които са в процес на обработване, както и всякаква налична информация за техния произход, освен когато тя е защитена от закон тайна;
- Да поиска коригиране на неточните лични данни, свързани с него, както и допълване на непълните лични данни;
- Да поиска изтриване на личните данни, които го засягат, когато обработването нарушава разпоредбите на ЗЗЛД;

- Да поиска ограничаване на обработването им, без да бъдат изтрити, когато точността на личните данни се оспорва от субекта на данните и това не може да се провери или личните данни трябва да се запазят за доказателствени цели;
- Преди премахването на ограничаването на обработването, администраторът е длъжен да информира субекта на данните;
- Да бъде писмено информиран, когато администраторът отказва да коригира, допълни, изтрие или ограничи обработването на лични данни;
- Да подаде жалба до Инспектората на Висшия съдебен съвет, както и да търси защита по съдебен ред;
- Упражняването на правата на субекта на лични данни, 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.

ПРБ предоставя информацията по начина на постъпване на искането. Когато това е невъзможно или изисква несъразмерно големи усилия, информацията се предоставя по друг подходящ начин, включително по електронен път. ПРБ отговаря на искането на субекта на данни или го информира писмено за действията, предприети във връзка с неговото искане, в срок до два месеца от получаване на искането. Срокът може да се удължи с още един месец, когато това се налага заради сложността или броя на исканията.

Начини за връзка с ПРБ

За упражняването на права, свързани с обработването на лични данни от Прокуратурата на Република България като орган на съдебна власт, субектите на данни могат да подадат своите искания по някой от посочените начини:

- Като изпратят своето искане за упражняване на права в писмена форма на адрес: гр. София 1061, бул. "Витоша" № 2;
- Като подадат лично своето искане за упражняване на права на адрес: гр. София 1061, бул. "Витоша" № 2;
- Като изпратят своето искане за упражняване на права на електронна поща: prbcont@prb.bg. Писмото трябва да е подписано с електронен подпис.

Право на жалба до Инспектората към Висшия съдебен съвет

Правото на жалба на субектите на данни се упражнява чрез подаването ѝ до надзорния орган Инспекторат към Висшия съдебен съвет: гр. София, п.к. 1000, ул. "Георг Вашингтон" №17, тел. деловодство - 02 9057550, факс: 02 9057503, ivss@inspectoratvss.bg, http://www.inspectoratvss.bg/

Първи етап на оценка на риска

Проверете дали дейността по обработване попада в списъка на Комисията за защита на личните данни (КЗЛД) за дейности при които се изисква изрично Оценка на въздействието върху защитата на данните (ОВЗД):

1. Мащабно обработване на биометрични данни за целите на уникалната идентификация на физическо лице, което не е спорадично.

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

2. Обработване на генетични данни с цел профилиране, което поражда правни последици за субекта на данни или по подобен начин го засяга в значителна степен.

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

3. 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.

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

4. Наличие на 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.

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

5. 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.

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

6. 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.

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

7. Обработване на лични данни на деца при пряко предлагане на услуги на информационното общество.

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

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

НЕ – продължете оценката на риска

ДА – извършете оценка на въздействието.

Втори етап на оценка на риска:

Първоначален анализ на риска

Прегледайте съответната дейност по обработване на лични данни дали се отнася към някоя от следните категории:

Критерии за проверка:

Критерии:	Пример	Мерки
Оценка или точкуване;	Например обработвате лични данни, на основата на които се правят изводи за някакви аспекти на личността субекта на данни – оценяване на резултати, образователен, професионален статус и т.н	Ако съществува –предпоставка за ОВЗД
Автоматизирано вземане на решения с правни последици или подобни сериозни последици;	Взимане на решение на базата само на автоматизирана обработка на данни през някакъв софтуерен механизъм, без право на субекта да има човешка намеса.	Ако съществува –предпоставка за ОВЗД
Систематично наблюдение;	Пример за такова е видеонаблюдението на публично достъпна зона. Също така може да има такова и в интернет мрежата, където е възможно доставчик да има от субекта редовна информация за: GPS данни, предпочитания към стоки, предпочитания към определени културни събития – книги, филми и т.н.	Ако съществува –предпоставка за ОВЗД
Чувствителни данни или данни от изключително лично естество;	определени в член 9 от ОРЗД (например информация относно политическите възгледи на физическите лица), както и лични данни, свързани с присъди и нарушения по смисъла на член 10. Тук може да има и други – всички данни свързани с личния живот на субекта, които	Ако съществува –предпоставка за ОВЗД

	той не е огласил публично – лична кореспонденция, лични връзки и т.н.	
Мащабно обработване на данни;	Пример са големите доставчици на интернет и комуникационни услуги, които могат да имат както данните на много на брой субекти, така и разнообразни.	Ако съществува –предпоставка за ОВЗД
Търсене на съвпадение или съчетаване на набори от данни;	Пример са т.нар. колектори на данни – например вземат се данни от открити държавни регистри и се съчетават, като към това съчетаване се прикрепят и данни от закрити източници.	Ако съществува –предпоставка за ОВЗД
Данни относно уязвими субекти на данни;	Уязвимите субекти на данни могат да включват деца (може да се счита, че те не са в състояние съзнателно и мотивирано да възразят срещу или да се съгласят с обработването на техните данни), по-уязвими сегменти от населението, които се нуждаят от специална защита (психично болни лица, търсещи убежище лица или възрастни лица, пациенти и др.)	Ако съществува –предпоставка за ОВЗД
Иновативно използване или прилагане на нови технологични или организационни решения;	Например някакъв вид контрол като се разпознават лица или друг вид биометрични данни.	Ако съществува –предпоставка за ОВЗД
Когато операциите по обработването сами по себе си „възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор".		Ако съществува –предпоставка за ОВЗД

В повечето случаи администраторът може да заключи, че ако обработването отговаря на два критерия, ще се изисква извършването на ОВЗД. Като цяло, на колкото повече критерии отговаря обработването, толкова по-вероятно е да поражда висок риск за правата и свободите на субектите на данни, поради което ще изисква ОВЗД независимо от мерките, които администраторът планира да въведе.

При все това в някои случаи администраторът може да заключи, че обработване, което отговаря само на един от тези критерии, изисква ОВЗД.

Примери за илюстрация: Виж Приложение №1

Вторичен анализ на риска

Вторичният анализ на риска е процес, при който оценката, дали да се прави ОВЗД е вторична – само ако рискът е висок.

Вторичния анализ се прави с цел да се оцени нивото на риск спрямо нивото на вероятност и степента на въздействие общо за дейността. Тази оценка на риска представлява анализа, който е необходим, за да се прецени нивото на адекватност на техническа и организационна защита на личните данни, както е и референтна стойност, която следва да се следи от администратора за управлението на риска като динамична стойност.

При оценката на риска администраторът да използва следната матрица за степенуване на въздействието (риска), отчитаща вероятността за настъпване на съответното нарушение на сигурността на данните и величината на потенциалните неблагоприятни последици (вреди):

Таблица 1

Риск – R		Последици			
		Ограничени	Средни	Тежки	Много тежки
Вероятност	Малка	Ниско - 1 -	Средно - 4 -	Средно - 6 -	Високо - 10 -
	Средна	Ниско - 2 -	Средно - 5 -	Високо - 8 -	Изключително високо - 11 -
	Висока	Средно - 3 -	Високо - 7 -	Високо - 9 -	Изключително високо - 12 -

Необходимо е да се анализира рискът относно дейността в три основни хипотези:

- Достъп до данните от обработването;
- Коригиране/модификация на данните от обработването;
- Заличаване/изтриване на данните от обработването.

Пример:

Дейност по обработване на данни на служители, при което те се изнасят на външен подизпълнител като му се пращат периодично на некриптирани файлове по електронна поща.

Достъп до данните от обработването:

Вероятността е висока поради незащитен канал и файлове за комуникация, последиците спрямо вида на данните е средна –оценката на риск е Висока-7

Коригиране/модификация на данните от обработването;

Вероятността е средна – възможно е да бъдат прехванати и подменени, но не е ограничена степента на риск, тъй като промяната на данните не би довело до нарушение на права и свободи -оценката на риск е Ниско – 1

Заличаване/изтриване на данните от обработването.

Вероятността от изтриване/заличаване на данни е ниска – администратора си разполага с копие, последиците биха били ограничени - 1

Не е необходима оценка на въздействието на цялата дейност, необходима е преценка на администратора и действия по какъв начин може да намали вероятността за настъпване на риск при хипотезата ***Достъп до данните за обработването*** и как може да я намали.

Хипотеза/Сценарий	Вероятност	Степен /Последици	Общо за риска
Достъп до данните от обработването;	Висока	Средни	Висока
Коригиране/модификация на данните от обработването;	Средна	Ограничена	Ниско
Заличаване/изтриване на данните от обработването.	Ниска	Ниска	Ниско

За да е възможно изготвянето на оценка на риска за всяка една дейност по отделно е необходимо всеки отдел и дирекция, отговарящ за процесите и дейностите в тяхната компетенция, да попълни предварително таблицата от Приложение 2 . Посредством събраната информация може да се премине към анализ на риска в трите хипотези. Може да се използва и информацията от Регистъра на дейностите по обработване, която в голяма степен съвпада.

Приложение № 1

Примери за обработване	Евентуално приложими критерии	Има ли вероятност да се изисква ОВЗД?
обработване на генетични и здравни данни	- Чувствителни данни или данни от изключително лично естество. - Данни относно уязвими субекти на данни. - Мащабно обработване на данни.	ДА
Използване на система от камери за наблюдение на поведението на шофьорите на магистралите. Администраторът предвижда да използва интелигентна система за видеоанализ за идентифициране на отделни автомобили и автоматично разпознаване на регистрационни номера.	- Систематично наблюдение. - Иновативно използване или прилагане на технологични или организационни решения.	
Дружество, което осъществява систематично наблюдение на дейностите на своите служители, включително наблюдение на работните станции на служителите, дейността им в интернет и др.	- Систематично наблюдение. - Данни относно уязвими субекти на данни.	
Събиране на публични данни от социални мрежи с цел изготвяне на профили.	- Оценка или точкуване. - Мащабно обработване на данни. - Търсене на съвпадение или съчетаване на набори от данни.	

	- Чувствителни данни или данни от изключително лично естество:	
Институция, която създава база данни за кредитен рейтинг или за борба с измамите на национално равнище.	- Оценка или точкуване. - Автоматизирано вземане на решения с правни последици или подобни сериозни последици. - Възпрепятства субект на данни да упражнява дадено право или да използва някоя услуга или договор. - Чувствителни данни или данни от изключително лично естество: - Чувствителни данни.	
Съхранение с цел архивиране на псевдонимизирани чувствителни лични данни относно уязвими субекти на данни, които са участвали в научноизследователски проекти или клинични изпитвания	- Данни относно уязвими субекти на данни. - Възпрепятства субекти на данни да упражняват дадено право или да използват някоя услуга или договор.	
Обработване на „лични данни на пациенти или клиенти на отделен лекар, друг здравен работник или адвокат" (съображение 91 от ОРЗД).	- Чувствителни данни или данни от изключително лично естество. - Данни относно уязвими субекти на данни.	НЕ
Онлайн списание, което използва списък с адресати, за да изпраща общо резюме с информация на своите абонати.	- Мащабно обработване на данни.	
Уебсайт за електронна търговия, на който се показват реклами за части за стари модели автомобили, което включва ог-	- Оценка или точкуване.	

раничено профилиране въз основа на разглежданите или закупените артикули на самия уебсайт.		

Приложение № 2

1	Име на дейност, контекст, описание	
2	Цел на дейността, начин на извършване	
3	Използвани видове данни за дейността (изброяване)	
4	Въведени и приложими за дейността технически мерки	
5	Въведени и приложими за дейността организационни мерки	
6	Спомагателни/поддържащи активи (supporting assets)	
7	Предаване на данни (начин на движение на поток от данни)	
8	Местоположение на данни (начин на съхранение)	
9	Роли и отговорности (кой има достъп до данните)	

Трети етап – ОВЗД и документиране

Използваната насока за изграждане на методологична рамка при ОВЗД е съобразена с препоръките на Европейският комитет по защита на данните (по-специално припознатите от Работна група по чл. 29) и добрите практики на френския надзорен орган (https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides).

1. Общ преглед

(Цел: да се получи ясен преглед на разглежданите операции по обработка на лични данни)

➢ **Описание на дейността;**

- *Обхват и естество на дейността; целите, за които е предназначено обработването; желаният резултат, който ще бъде постигнат;*

➢ **Описание на данните, цикълът на обработка и потоците от данни;**

- *Видовете данни, които участват в обработването; източниците и получателите на данни; общите срокове на съхранение;*

➢ **Спомагателните активи, участващи в процесите по обработка;**

- *Описание/изброяване на активите през целия цикъл на обработка на данните;*

2. Описание на планирани/съществуващи мерки

(Цел: изграждане на система, която гарантира спазването на принципите за защита на личните данни)

➢ **Правни мерки** - описание как се спазват принципите на ОРЗД, описание как се спазват правата на субектите и др.

- *Правна защита при участващи обработващи (трети страни); защита при трансфер на данни извън ЕС*
- *Оценка на контрола, гарантиращ принципите на пропорционалност и необходимост от обработката*
- *Оценка на контрола за защита на правата на субектите на данни по отношение на :*
  - *Информираност;*
  - *Събиране на данни от субекта чрез съгласие;*
  - *Правото на достъп и правото на преносимост;*
  - *Правото за коригиране и изтриване;*
  - *Правото за ограничаване и правото на възражение*

➢ **Технически мерки** – описание на софтуерни и хардуерни спецификации и др.
➢ **Физически мерки** – правила за физически достъп до помещения, мерки за противопожарна безопасност и др.

- *Оценка на техническите и физически мерки в следните предназначения:*
  - *Специфични технически контроли за обработването;*
  - *Общи правила и технически контроли за инфраструктурата;*
  - *Организационни мерки за обработването и инфраструктурата.*

3. Риск- Оценка на риска: потенциални нарушения на личните данни

(Цел: постигане на добро разбиране на причините и последствията от рисковете)

Изготвя се обобщен анализ на базата на единни параметри в три хипотези:

- Анализ на хипотеза № 1- **Достъп до данните**;
- Анализ на хипотеза № 2- **Модификация на данните**;
- Анализ на хипотеза № 3 - **Заличаване на данните**;

Параметри:

- Идентифициране на **потенциалните вреди** за субектите на данни;
- Определяне на **степента** за нарушение на правата и свободите на лицата (до каква степен са засегнати/нарушени);
- Идентифициране на **заплахите** и **източниците** на риск към съответните спомагателни активи;
- Определяне на **вероятността** в зависимост от уязвимостта на спомагателните активи за достъп , контрол и модификация;

4. Валидация

(Цел: да се реши дали да се приеме ОВЗД на база констатациите от анализа)

- Изготвя се картографиране на риска, което може да бъде проследено заедно с бъдещи мерки, които да въздействат на риска;
- Изготвя се план за действие, който има за цел да въведе конкретните механизми за понижаване на риска;
- Изготвят се мнения и препоръки от ДЛЗД;
- Формално одобрение на ОВЗД в следните варианти:
  - Валидирано
  - Необходимо е подобрение (връщане към стъпка № 2)
  - Отхвърлено (преминаване към стъпка № 6)

5. Изготвяне на резюме за оценка на риска и въздействието

(Цел: да послужи като отчетна форма за предприетите мерки към регистъра по чл. 30)

Изготвянето на обобщено резюме при направена оценка на въздействието може да се представя в следния вариант:

След направената, одобрената/върната за подобрение/отхвърлена валидация на ОВЗД се установи:

1. *Нивото на риск за дейността е (описание на риска от анализа), което е управляемо/не достатъчно поради наличието на (описание на причините от анализа).*
2. *Предприети са мерки за подобрение при управлението на риска при (посочване на хипотезите от анализа на риска/правните мерки)*
3. *Изготвен е план за действие и създадени препоръки на ДЛЗД , които ще доведат до намаляване на нивото на риск до желаното по отношение на (посочване обектите)*
4. *Дейността отговаря на изискванията на ОРЗД/ Необходимо е /Не е допитване до надзорен орган планиран следващ преглед на дейността на (дата) или до промяна, налагаща извършване на повторно ОВЗД.*

Съставил: *Одобрил:*

Дата: *Дата:*

6. Последици от ОВЗД

Когато оценката на въздействието върху защитата на данните съгласно член 35 от ОРЗД и чл. 64 от ЗЗЛД покаже, че обработването ще породи висок риск въпреки предприетите от администратора мерки за ограничаване на риска, то:

- Администраторът следва да се откаже от предприемане на този вид обработване или
- Да проведе предварителна консултация с надзорния орган преди започване на обработването.

Съхранение и отчетност на записите на дейностите, за които е извършено ОВЗД

Съхраняване

Всеки извършен анализ на ОВЗД се съхранява и поддържа на хартиен и електронен носител (.json формат към софтуерното приложение) носител, подробно включващ описанието на всяка стъпка от методологията и е неразделна част от вътрешната документация на администратора, приложим към регистъра по чл. 30.

Отчетност

При поискване от надзорния орган задължението за предоставяне и разяснение на ОВЗД е на длъжностното лице по защита на данните.

Приложение № 11
Политика за защита на личните данни

ПРОТОКОЛ
ЗА УНИЩОЖАВАНЕ НА МАТЕРИАЛНИ НОСИТЕЛИ, ИЗПОЛЗВАНИ ЗА ЗАПИС НА ЛИЧНИ ДАННИ

Структурно звено	…….. (Посочете структурното звено, в което е извършено унищожаването)
Описание на носителите за многократен запис	…… (Посочете вида на носителя, например флаш памет, диск, дискета, както и броя на унищожените носители)
Причина за унищожаването	…… (Посочете причината за унищожаване, например техническа повреда, носител за еднократен запис, както и броя на унищожените носители)
Звено, от което е получен носителят	…… (Посочете звеното/звената, от които са получени носителите за унищожаване)
Преглед и изтриване на личните данни от носителя преди унищожаването	…… (Посочете дали при извършения преглед са налични лични данни в носителя и дали са предприети действия по тяхното изтриване преди унищожаване на носителя. В случай на унищожаване поради техническа повреда, която прави невъзможен прегледа на носителя, отбележете „Невъзможно“.)
Забележка	…… (Посочете други обстоятелства, които са относими към конкретната дейност по унищожаване)
Дата на унищожаване и протоколиране	……
Извършил унищожаването	…… (Име, длъжност и подпис на лицето, извършило унищожаването, респ. на членовете на комисията, на която е възложено унищожаването и номер на заповед за създаване на комисията)
Съгласувал:	…… (Дата, име и подпис на .....)

ОБРАЗЕЦ НА ФОРМА ЗА ОТТЕГЛЯНЕ НА СЪГЛАСИЕ ОТ СУБЕКТА НА ДАННИТЕ

Аз, долуподписан/ият/та ,

.....

(три имена на субекта на данните, друга информация за идентификация и контакти),

в качеството си на „субект на лични данни" и при условията на Общия регламент относно защитата на данните,

като се има предвид, че:

съм предоставил съгласието си за обработване на следните лични данни:

.....

(посочва се точно за какви лични данни е дадено съгласие)

по следния начин:

.....

(посочва се по какъв начин е дадено съгласието - на хартиен формуляр, по електронен път и т.н.),

във връзка със следната цел:

.....

(изрично уточнете целите, които са декларирани при даване на съгласие за обработването на тези лични данни)

от администратора на лични данни Прокуратура на Република България, 1061 София, бул. „Витоша" № 2;

.....

(име на администратора, данни за идентификация)

и като заявявам, че съм надлежно информиран, че имам право да оттегля съгласието си за обработване на лични данни частично или изцяло по всяко време, без да съм задължен да посочвам причина за оттеглянето.

С НАСТОЯЩОТО ВИ УВЕДОМЯВАМ, ЧЕ:

Оттеглям съгласието си личните ми данни, посочени в това уведомление, да бъдат събирани и обработвани за посочената цел/цели.

Декларирам, че оттеглям своето съгласие за обработване на лични данни свободно, изрично и относно всички посочени лични данни, съгласно собствената си воля и убеждение.

Запознат съм, че имам право на възражения и жалби пред Комисия за защита на личните

данни, която е надзорен орган в Република България относно прилагането на Общия регламент, в случай че администраторът на лични данни продължи обработването на горепосочените данни след оттеглянето на съгласието с настоящото уведомление.

Дата: Подпис:.....

Получено от:.....на.....

ПРОЦЕДУРА ЗА НАЧИНИТЕ НА КОМУНИКАЦИЯ ПРИ ЖАЛБИ И ЗАЯВЛЕНИЯ (ИСКАНИЯ) ОТ СУБЕКТА НА ДАННИ

I. Предназначение на процедурата

Тази процедура се отнася до:

- начините и средствата, с които субектите на данни могат да отправят заявления и жалби, свързани с обработването на техните лични данни от Прокуратурата на Република България;
- обработка на заявления/искания от субектите на данни относно упражняването на техните права по Общия регламент за защита на данните (ОРЗД);
- жалби на субектите на данни относно начина на обработване на техните искания или жалби.

II. Нормативна уредба

- Член 12 от Общия регламент за защита на данните (ОРЗД)
- Членове 37б, 37в и 38 от Закона за защита на личните данни (ЗЗЛД)
- Насоки относно прозрачността съгласно Регламент 2016/679

III. Задължения и роли

Всички служители в Прокуратурата на Република България, които по силата на служебните си задължения получават и приемат жалбите/исканията по упражняване на правата по ОРЗД, направени от субекти на лични данни са длъжни да се запознаят и спазват настоящата процедура.

IV. Ход на процедурата

1. Обща информация и съобщения

Заявление (искане) може да бъде подадено по следните начини:

- чрез писмено заявление до Администратора или определените от него лица или
- по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация;

Прокуратурата на Република България обявява координатите за контакт със своето Длъжностно лице по защита на данните, като ги публикува на своята интернет страница на адрес www.prb.bg , ясно обособени в секцията "Защита на личните данни".

Прокуратурата на Република България поставя ясни и разбираеми указания на интернет страницата си относно подаването на искания и жалби, както и примерна форма за искания на субектите на данни (виж Образец на форма за заявление (искане) от субект на данните *(Приложение № 18)*.

ПРБ предоставя публичен достъп на субектите на данните до своята Декларация за поверителност (уведомление за поверително третиране на личните данни) *(Приложение № 9)*, като я публикува на своя уеб сайт, така че да е ясно видима в секцията "Защита на личните данни" и да е достъпна при попълването на електронната форма за подаване на искания и жалби.

ДЛЗД и административните ръководители на прокуратури или оправомощените от тях служители документират всички действия във връзка с комуникацията със субектите на данни в Дневник на исканията.

2. Възможности на субекта на данни

Субектите на данни могат да подадат до Администратора:

- искания за осъществяване на правата им по защита на личните данни – искане за достъп, за изтриване, за ограничаване на обработването, възражение за обработване, за пренос на данните;
- възражения относно начина на разглеждане на искането/жалбата им;
- жалба срещу всяко решение, взето след подадено искане/жалба.

3. Начин на подаване на искания и жалби

Субектите на данни могат да отправят заявление за упражняване на своите права по ОРЗД чрез Образец на форма за заявление (искане) от субект на данните *(Приложение № 18)*.

В случай, че лицето желае да подаде заявление за упражняване на своите права по ОРЗД лично, то се обработва според правилата на „Инструкцията за деловодната дейност и документооборота в прокуратурата на РБ".

4. Отговор и срокове

Администраторът разглежда и взема решение по постъпилото искане или жалба при спазване на следните правила и срокове:

- Исканията/жалбите се насочват към определените от главния прокурор лица, които трябва да вземат решение и да дадат отговор на субекта на данните най-късно в срок от един месец от тяхното получаване;
- Администраторът (ръководителите на структурни звена с право на достъп до лични данни) изготвя отговор на исканията/жалбите на субектите на данни като взима предвид, при необходимост, становището и/или проекта на отговор изготвени от Длъжностното лице по защита на данните.
- Ако Администраторът не удовлетвори искането на субекта на данни в рамките на изискуемите срокове или откаже да уважи жалбата, то в отговора си излага на ясен и разбираем език причините, поради които не е предприел действие или е отказал.
- Администраторът също така информира в отговора си субекта на данните относно тяхното право да подават жалби директно до надзорния орган, като едновременно с това предоставя на субекта на данните координатите за контакт с надзорния орган и ги информира за правото им да търсят правна защита.

Всички действия на Администрация на Главния прокурор, предприети в изпълнение на настоящата процедура, се извършват без да се дължи заплащане от субекта на данните.

V. Примерни образци

- Образец на форма за заявление (искане) от субект на данните *(Приложение № 18);*
- Декларация за поверителност (уведомление за поверително третиране на личните данни) *(Приложение № 9);*
- Съобщение за условия за използване на бисквитки *(Приложение № 25).*

ПРИМЕРНИ КЛАУЗИ ЗА ПОВЕРИТЕЛНО ТРЕТИРАНЕ НА ЛИЧНИТЕ ДАННИ КЪМ ДОГОВОРИ МЕЖДУ АДМИНИСТРАТОРИ

.....

Глава (n)

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

чл. (n). Двете страни по настоящия договор декларират, че са запознати с Регламент (ЕС) 2016/679 за защита на личните данни и в ролята си на администратор на лични данни са въвели в своите организации необходимите мерки за съответствие с неговите изисквания.

чл. (n). Двете страни се задължават да третират всички лични данни на другата страна, които ще им станат известни в процеса на изпълнение на договора, като поверителни и да не ги разкриват, освен на служителите си и обработващи подизпълнители, и само доколкото това е необходимо за изпълнение на дейностите по договора.

чл. (n). Двете страни се задължават да използват личните данни, получени или станали им известни от другата страна, само за целите на изпълнение на настоящия договор и използването на данните за каквито и да е други цели от една от страните ще бъде нарушение на настоящия договор спрямо другата, изправна страна.

чл. (n). В случай на нарушение на сигурността на личните данни, като резултат от виновно неизпълнение на поетите задължения относно поверителното третиране на личните данни по настоящия договор, виновната страна носи пълна имуществена отговорност пред изправната, включително и за наложени й санкции от надзорните органи по защита на данните.

.....

ПРИМЕРНИ КЛАУЗИ ЗА ПОВЕРИТЕЛНО ТРЕТИРАНЕ КЪМ ДОГОВОР С ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Глава (n)

ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

чл. (n). Настоящата глава от договора, съгласно Регламент (ЕС) 2016/679 за защита на личните данни, наричан по-нататък за краткост Общия регламент, е във връзка със задължението на Възложителя и Изпълнителя да сключат писмен договор, с който да уговорят правата, задълженията и отговорностите на страните във връзка с личните данни, които Изпълнителят обработва от името на Възложителя.

чл. (n). По смисъла на Общия регламент Възложителят е в качеството си на администратор на лични данни, а Изпълнителят е в качеството си на обработващ на лични данни, а физическите лица, чийто данни се обработват, се наричат субекти на данни.

чл. (n). Обработващият се задължава 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.

С настоящият договор двете страни се съгласяват че:

- на обработващият се забранява да използва от своя страна подизпълнители за обработването на личните данни без изрично писмено разрешение от администратора.
- В случаите, когато на обработващия бъде разрешено да превъзложи обработването на лични данни на подизпълнител, то той 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;
- Договорите с подизпълнители от второ ниво се одобряват, само ако изискват от тях да спазват най-малко същите разпоредби за сигур-

ност и другите изисквания, които се отнасят и до организацията на обработващия.

- При прекратяването на договор с обработващия или негови подизпълнители, съответните лични данни трябва да бъдат унищожени или върнати на администратора по веригата от подизпълнители.

чл. (n). (1) Изпълнителят, в ролята си на обработващ, гарантира на Възложителя, като администратор на лични данни, че е предприел и прилага следните организационни и технически мерки:

1. внедрена е цялостна система от политики, правила и процедури за обработка на лични данни, в т.ч. в качеството на обработващ на лични данни на субекти на данни, които са служители, клиенти или доставчици на администратори на лични данни, от чието име се обработват лични данни;
2. всички лица, които са под ръководството на Изпълнителя и които са оправомощени да обработват лични данни от името на администратора, са обучени по внедрената система от политики и процедури и са поели ангажимент за поверителност на обработваните лични данни;
3. извършени са оценки за нивото на въздействие в случай на нарушаване сигурността на обработвани от името на Възложител лични данни, по отношение на рисковете с различна вероятност и тежест за правата и свободите на субектите на данни и всички внедрени организационни и технически мерки за защита на личните данни съответстват на тези оценки;
4. внедрени са и приложени достатъчни организационни и технически мерки за ограничаване и регламентиране на достъпа до и обработката на физически и електронни носители на лични данни;
5. внедрени са и приложени достатъчни мерки за съхраняване на необходими за обработка лични данни и ред за преглед и унищожаване на ненужни лични данни;
6. внедрени са и приложени достатъчни мерки за съдействие при изпълнение задълженията на администратор, от чието име се обработват лични данни, при упражняване правата на субектите на данни, в т.ч. и своевременно уведомяване за всеки случай на нарушаване сигурността на личните данни;

7. внедрени са и са приложени достатъчни организационни и технически мерки за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
8. внедрен е процес за редовно изпитване, преценяване и оценка на ефективността на организационните и техническите мерки с оглед постоянно да се гарантира сигурността на обработването.

(2) Изпълнителят гарантира, че в резултат на посочените мерки, обработването на лични данни, които са предоставени за обработка от Възложителя на Изпълнителя, протича в съответствие с изискванията на Общия регламент и осигурява защита на правата на субектите на данни.

чл. (n). За всяко нарушение на сигурността на обработваните от името на Възложителя лични данни, което е по вина на Изпълнителя или негов подизпълнител, за които Възложителят е претърпял санкции и/или вреди, Изпълнителят носи пълна имуществена отговорност пред Възложителя.

Приложение № 16
Политика за защита на данните

ПРОТОКОЛ
ЗА ИЗВЪРШЕНА ПЕРИОДИЧНА ПРОВЕРКА
ПО ЧЛ. 46 ОТ ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Структурно звено	..... (Посочете структурното звено, в което е извършена проверката)
Период на проверката	..... (Посочете периода от време, в който е извършена периодичната проверка)
Обхват на проверката	..... (Посочете личните данни, за които е извършена периодичната проверка, чрез описание на рег. № на преписка, материал или друг носител)
Преценка относно по-нататъшното съхранение на личните данни	..... (Преценката може да бъде за унищожаване на всички проверени материали, унищожаване на част от проверените материали и продължаване съхранението на друга част от проверените материали)
Мотиви за продължаване на съхранението	..... (Посочете мотиви за продължаване на съхранението, например: за да не се допусне възпрепятстването на проверки, разследвания или процедури; за да не се допусне неблагоприятно засягане на предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания; за да се защити обществения ред и сигурност; за да се защитят правата и свободите на други лица)
Срок за извършване на следващата периодична проверка	..... (Посочете период за извършване на следваща проверка, който не може да бъде по-дълъг от 3 години)
Забележка	..... (Посочете други обстоятелства, които са относими към дейността по проверката или могат да имат значение за следващата проверка)
Дата на изготвяне на протокола	.....
Извършил проверката	..... (Име, длъжност и подпис на лицето, извършило проверката, респ. на членовете на комисията, на която е възложена проверката и номер на заповед за създаване на комисията)

ДОГОВОР ЗА ОБРАБОТВАНЕ НА ДАННИ МЕЖДУ АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ И ОБРАБОТВАЩ

Днес,....., между страните:

1. ....., ЕИК..... , седалище и адрес на управление..... , представлявано от ....., наричано в договора, АДМИНИСТРАТОР

И

2. ....., ЕИК..... , седалище и адрес на управление..... , представлявано от .....(ако е физическо лице се индивидуализира с ЕГН, адрес), наричано в договора, ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Дефиниции:

1. „Администратор" на лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на ЕС или в правото на държава членка.

2. „Обработващ лични данни" означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора

3. „Обработване на лични данни" е 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

Като се има предвид че:

• АДМИНИСТРАТОРЪТ има достъп до личните данни на следните физически лица *(служители, ...)* ..... наричани по-долу "субектите на данни", като обработването на личните данни е във връзка със следната цел: .....

• АДМИНИСТРАТОРЪТ желае ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ да извърши определени видове обработване в съответствие с настоящото споразумение.

• АДМИНИСТРАТОРЪТ е определил целта и средствата за обработване на лични данни, а именно: .....

• ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ се е задължил да се съобрази с настоящото споразумение за обработване на данни и да спазва задълженията за сигурност и защита на лични данни съгласно Общия регламент относно защита на данните.

• АДМИНИСТРАТОРЪТ се счита за отговорна страна по смисъла на Общия регламент

Страните се споразумяха за следното:

I. СРОК НА ДОГОВОРА

Чл.1.Договорът се сключва за .....срок

II. ЦЕЛИ НА ОБРАБОТВАНЕТО

Чл.2.Обработващият лични данни се задължава да обработва лични данни от името на Администратора в съответствие с целта и условията, определени в настоящото споразумение за обработване на данни, както следва: .....

Чл.3.(1) Обработващият лични данни се съгласява да се въздържа от използването на личните данни за каквато и да е друга цел, различна от посочената от Администратора.

(2) Администраторът на лични данни се задължава да информира обработващия лични данни преди всяко обработване за цели, които не са предвидени в това Споразумение за обработка на данни.

Чл.4.Обработващият лични данни обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на ЕС или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес

III. ЗАДЪЛЖЕНИЯ НА ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ

Чл.5.(1) Обработващият лични данни:

а) гарантира, че лицата, оправомощени от него да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

б) взема всички необходими мерки съгласно член 32 от Общия регламент във връзка със сигурността на обработването на личните данни;

в) подпомага Администратора да гарантира изпълнението на задълженията съгласно членове *32 - 36* от Общия регламент, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;

г) по избор на Администратора заличава или връща на Администратора всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на ЕС или правото на държава членка не изисква тяхното съхранение;

д) осигурява достъп на Администратора до цялата информация, необходима за доказване на изпълнението на задълженията, и позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг одитор, оправомощен от Администратора. Обработващият лични данни незабавно уведомява администратора, ако според него дадено нареждане нарушава Общия регламент или други разпоредби на ЕС или на държавите членки относно защитата на данни;

е) спазва необходимите условия за включване на друг обработващ лични данни;

ж) подпомага Администратора, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задълженията му;

з) по избор на Администратора заличава или връща на администратора всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза или правото на държава членка не изисква тяхното съхранени;

и) осигурява достъп на Администратора до цялата информация, необходима за доказване на изпълнението на задълженията и позволява и допринася за извършването на одити, включително проверки, от страна на Администратора или друг одитор, оправомощен от него. Обработващият лични данни незабавно уведомява администратора, ако според него дадено нареждане нарушава изискванията на Общия регламент или други разпоредби на ЕС или на държавите членки относно защитата на данни;

ж) Обработващият лични данни може[1] в рамките на настоящото споразумение да ангажира друг обработващ лични данни при следните условия ....., като гарантира, че избраният от него обработващ лични данни се е съгласил писмено със същите задължения, които са съгласувани между администратора и обработващия лични данни.

з) В случай на договореност с администратора, обработващият може да уведоми надзорния орган за нарушения на личните данни от името на администратора, ако администраторът е дал на обработващия разрешение и това е част от договорните споразумения между администратора

IV. РАЗПРЕДЕЛЕНИЕ НА ОТГОВОРНОСТТА

Чл.6.(1) Обработващият лични данни е отговорен само за обработката на личните данни съгласно настоящото споразумение за обработка на данни, в съответствие с инструкциите на администратора и на контролиращия орган.

(2).Обработващият лични данни гарантира, че има изрично съгласие и / или правна основа за обработка на съответните лични данни. Освен това гарантира, че съдържанието на личните данни и обработката не е незаконно и не нарушава правата на трета страна.

V. ЗАДЪЛЖЕНИЕ ЗА ДОКЛАД

Чл.7.(1) В случай на изтичане на данни или друго нарушение съгласно Общия регламент, обработващият лични данни трябва да уведоми администратора за това без забавяне, след което администраторът информира субектите на данни и съответния надзорен орган.

(2) Във връзка с ал.1, обработващият лични данни се задължава да предостави пълна и точна информация.

(3) Обработващият лични данни се задължава да си сътрудничи със съответните органи, включително надзорни органи и / или субектите на данни, като остава отговорен за неизпълнение на законовите си задължения.

(4) Задължението за докладване включва във всеки случай задължението да докладва и фактът, че е настъпило .....*(изтичане на данни/друго нарушение)*, включително подробности относно .....*(предполагаемата причина)*; известните и / или очаквани последствия, предложеното решение, мерките, които са предприети.

VI. СИГУРНОСТ

Чл.8.Обработващият лични данни се задължава да предприеме подходящи технически и организационни мерки във връзка със защитата на личните данни, като

.....
.....

Чл.9.(1) За да се потвърди спазването на настоящото споразумение за обработване на данни, Администраторът има право да извърши одит, който има право да възложи и на независима трета страна, за което следва да уведоми писмено обработващия лични данни. Одитът може да бъде извършен при .....*(напр. конкретни основания за злоупотреба с лични данни)*, не по-рано от .....дни от ....., след като администраторът е уведомил писмено обработващия лични данни.

(2) Констатациите по отношение на извършения одит ще бъдат обсъдени и оценени от страните.

(3) Разходите за одита ще бъдат поети от .....

VII. ИЗМЕНЕНИЕ.ПРЕКРАТЯВАНЕ

Чл.10.(1) Настоящото Споразумение за обработване на данни се сключва за срока, посочен в чл.1.

(2) Споразумението за обработване на данни може да бъде прекратено:

- с изтичане на срока;
- по взаимно съгласие, изразено писмено;
- при неизпълнение на задълженията на всяка от страните, както и при нарушения на Общия регламент, като в този случай всяка от страните има право да уведоми надзорния орган за извършеното нарушение.

Чл.11.Настоящото споразумение за обработване на данни може да бъде изменяно само от страните по взаимно съгласие.

VIII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл.12.(1) Споразумението за обработване на данни и тяхното прилагане ще се регулира от .....(българското) законодателство.

(2) Всеки спор, възникващ между страните по отношение на и / или произтичащ от настоящото споразумение за обработване на данни, ще бъде отнесен до компетентния орган.

Настоящото споразумение беше съставено в .....екземпляра.

Администратор .....(подпис)

Обработващ лични данни .....(подпис)

Като неразделна част от договора, в отделно приложение, могат да бъдат изведени конкретно:

- категориите субекти на данни;

- видовете лични данни;

- цел на обработването;

- мерките за сигурност на личните данни и др. съществени изисквания според конкретния случай.

[1] Администраторът на лични данни може и да ограничи правото на Обработващия да възлага обработването на данните от друг подизпълнител. Това е въпрос на конкретно споразумение.

Заявление (Искане) от:

Данни на физическото лице:	
Три имена	
ЕГН/ЛНЧ	
Ако сте чуждестранно физическо лице, моля посечете тук и датата си на раждане дд/мм/година	
Данни за контакт:	
Държава, населено място	п.к.
Настоящ адрес *жк.,ул.,№, бл. ет., ап.*	
E-mail	

Представител на субекта на данни:

Действате ли като представител от името на субекта на данни?	НЕ ☐ ДА ☐
Ако "Да", моля, посочете в качеството си на какъв (например родител, настойник, попечител, упълномощен представител)	
Три имена	
Дата на раждане	
Данни за контакт	
Държава, град	Пощенски код
Настоящ адрес	жк.,ул.,№, бл. ет., ап.
Допълнителни данни за идентификация на представителя:	*Моля, приложете доказателства[1], че сте законно упълномощени да получавате тази информация.*

Предпочитана форма за получаване на информация за искането:

[1] Например - пълномощно, удостоверение за назначаване на настойник/попечител и др.

Предпочитана форма за получаване на информация <u>при искане за достъп</u>:

☐ Преглед на информация	☐ Устна справка	☐ Писмена справка	☐ Копия на технически носител

Относно:

Искане за достъп *(получаване на информация за обработваните данни)*	ДА ☐
Искане за коригиране *(актуализиране на данни)*	ДА ☐
Искане за изтриване/заличаване на данни *(право да бъдеш забравен)*	ДА ☐
Искане за ограничаване на обработването *(обработване до конкретна цел)*	ДА ☐
Възражение срещу обработване *(право на възражение)*	ДА ☐
Искане за пренос на данни *(право на преносимост)*	ДА ☐
Описание на искането :	

2. ДЕКЛАРАЦИЯ

Аз, долуподписаният ....., като декларирам, че посочените по-горе данни са верни, с настоящото заявявам пред ПРБ искането ми, посочено по-горе, относно описаните данни.

Дата:

Подпис:

В случай на подаване на това искане по електронен път следва да бъде подписано с електронен подпис на подателя (субекта на данни/упълномощеното лице).

ОБРАЗЕЦ НА УВЕДОМЯВАНЕ НА ПОЛУЧАТЕЛИ НА ЛИЧНИ ДАННИ ПРИ КОРИГИРАНЕ

ДО

.....

УВЕДОМЛЕНИЕ
ОТНОСНО КОРИГИРАНЕ НА ЛИЧНИ ДАННИ НА
.....

УВАЖАЕМИ ГОСПОДИН/ГОСПОЖО .....

С настоящото Ви уведомяваме, че на основание чл. 16 от Регламент (ЕС) 2016/679 администраторът на лични данни ..... извърши коригиране на неточни данни, отнасящи се до ...../извърши коригиране чрез попълване на непълните лични данни, отнасящи се до ..... След корекцията точните данни, които следва да обработвате, са както следва: .....

.....

ОБРАЗЕЦ НА УВЕДОМЯВАНЕ НА ПОЛУЧАТЕЛИ НА ЛИЧНИ ДАННИ ПРИ ИЗТРИВАНЕ

ДО

.....

УВЕДОМЛЕНИЕ
ОТНОСНО ИЗТРИВАНЕ НА ЛИЧНИ ДАННИ НА
.....

УВАЖАЕМИ ГОСПОДИН/ГОСПОЖО .....

С настоящото Ви уведомяваме, че на основание чл. 17, пар.1, б. „....“ от Регламент (ЕС) 2016/679 администраторът на лични данни ..... изтри всички лични данни, отнасящи се до ....., свързани с ..... (посочват се категориите лични данни, които са изтрити, а не конкретните данни). Информираме Ви, че в резултат на това изтриване, Вие също следва да изтриете тези данни, които сме Ви предоставили/разкрили преди това

ОБРАЗЕЦ НА УВЕДОМЯВАНЕ НА ПОЛУЧАТЕЛИ НА ЛИЧНИ ДАННИ ПРИ ОГРАНИЧАВАНЕ НА ОБРАБОТВАНЕТО

ДО

.....

УВЕДОМЛЕНИЕ ОТНОСНО ОГРАНИЧАВАНЕ НА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ НА

.....

УВАЖАЕМИ ГОСПОДИН/ГОСПОЖО .....

С настоящото Ви уведомяваме, че на основание чл. 18, пар.1, б. „....“ от Регламент (ЕС) 2016/679 администраторът на лични данни ..... ограничи обработването на лични данни, отнасящи се до ....., свързани с ..... (посочват се категориите лични данни или конкретните данни, чието обработване е ограничено). Информираме Ви, че Вие също следва да ограничите обработването на тези данни, които сме Ви предоставили/разкрили, до отпадане на основанието за ограничаване, за което ще Ви информираме допълнително.

УВЕДОМЛЕНИЕ ОТ АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ ДО НАДЗОРНИЯ ОРГАН ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

УВЕДОМЛЕНИЕ

за нарушаване на сигурността на данните

на основание чл. 33 от Регламент (ЕС) 2016/679 (Общия регламент относно защитата на личните данни) или на основание чл. 67 от Закона за защита на личните данни

Този формуляр е примерен и е за нарушение на сигурността, което трябва да докладват на Комисията за защита на личните данни (КЗЛД).

1.Тип на уведомлението

1.1 Първоначално ДА ☐ НЕ ☐

(В случай че не е налице цялата информация за нарушението на данните и ще бъде представено без ненужна забавяне последващо уведомление. Ако е имало забавяне при докладването на това нарушение, моля обяснете защо.)

.....
.....

1.2 Последващо ДА ☐ НЕ ☐

(В случай, че това уведомление е последващо, моля, посочете № и дата на първоначално подаденото уведомление относно нарушението)

.....

2. За нарушението

2.1. Продължаващо нарушение ДА ☐ НЕ ☐

.....

2.2. Кога (начална дата и час) е настъпило нарушението:
.....

(Ако не знаете точните дата/час , моля, посочете приблизителни - година / месец / дата / час)

2.3. Кога (начална дата и час) е установено нарушението:
.....

(Ако не знаете точните дата/ час , моля, посочете приблизителни - година / месец / дата / час)

2.4. Моля, опишете как открихте/разбрахте за нарушението?

.....

2.5. Причини за неспазването на 72-часовия срок

.....

(Задължително се попълва, в случай че са изминали повече от 72 часа от узнаване за нарушението)

2.6. Дата на уведомяване от обработващия (ако е приложимо).....

(Ако не знаете точните дата/ час , моля, посочете приблизителни. Попълва се само в случай, че обработващият лични данни Ви е уведомил за нарушението на данните)

2.7. Коментари за датите.....

(По желание - можете да предоставите допълнителна информация относно датите на уведомяване, както и да посочите дали не са Ви известни точните дати, ако смятате, че е необходимо.)

3. Данни за нарушението

3.1. Описание на нарушението *(Моля, опишете какво се е случило)*

.....

3.2. Моля, опишете как е станал инцидентът?

.....

3.3. Моля, уточнете, според Вас, дали това е:

3.3.1. Нарушение на поверителността? ДА ☐ НЕ ☐

(Попълвате "ДА" в случай на неправомерно, преднамерено или случайно разкриване или достъп до лични данни. Това включва разкриване на лични данни пред (или достъп до тях на) получатели, които не са оправомощени да ги получат (или да имат достъп до тях), или всеки друг вид обработване, което е в нарушение на ОРЗД. неразрешено разкриване на данните или неоторизиран достъп до данните и т.н.)

И / ИЛИ

3.3.2.Нарушение на целостта? ДА ☐ НЕ ☐

(Попълвате "ДА" в случай на преднамерено или случайно повреждане на лични данни. „Повреждане“ е налице, когато личните данни са променени, подменени/преправени или са непълни.)

И / ИЛИ

3.3.3. Нарушение на наличността? ДА ☐ НЕ ☐

(Попълвате "ДА" в случай преднамерена или случайна загуба на данни, унищожаване на данни или неналичена услуга. „Загуба“ на лични данни е състояние, при което данните може да са все още налични, но администраторът на лични данни (АЛД) е загубил контрол или достъп до тях или вече не ги притежава. „Унищожаване“ на лични данни е налице, когато данните вече ги няма или ги няма във вид, в който може да бъдат използвани.)

4. Категории данни на физическите лица, засегнати от нарушението

Идентичност на физическите лица:

☐име;

☐ ЕГН;

☐ адрес;

☐ паспортни данни;

☐ месторождение;

☐ телефон;

☐ е-мейл

☐ други:.....

Биометрични и генетични данни:

☐ човешки геном;

☐ дактилоскопични отпечатъци;

☐ снимки на ретина;

☐ ДНК;

☐ хромозоми;

☐ други:.....

Икономическа идентичност:

☐ имотно състояние;

☐ финансово състояние;

☐ участие и/или притежаване на дялове или ценни книжа в дружества;

☐ други:.....

Семейна идентичност:

☐ семейно положение;

☐ родствени връзки;

☐ други: .....

Социална и културна идентичност:

☐ произход;

Лични данни, които разкриват:

☐ произход (расов, етнически)

☐ убеждения (политически, религиоз-

☐ образование;

☐ трудова дейност;

☐ среда;

☐ навици;

☐ интереси;

☐ хоби;

☐ други:.....

ни, философски)

☐ членство в политически партии, организации, сдружения с религиозни, философски, политически или синдикални цели

☐ сексуалния живот и/или сексуалната ориентация

☐ други: .....

☐ **Лични данни, които се отнасят до наказателни присъди и престъпления.**

☐ **Лични данни, които се отнасят до физическото и психическо здраве.**

☐ **Лични данни, които се отнасят до местоположение, например координати.**

☐ **Данни и/или съвкупност от гореизброените данни, които могат да послужат за профилиране.**

5. Брой записи на лични данни, засегнати от нарушението .....

6. Брой субекти на данни (физически лица), засегнати от нарушението .....

(Един и същи субект може да фигурира в няколко записа на данни и/или в един запис да се съдържат данни за повече от едно физическо лице)

7. Колко субекти на данни може да бъдат засегнати .....

8. Категории субекти на данни:

☐ служители/персонал

☐ потребители

☐ абонати

☐ клиенти

☐ контрагенти

☐ кандидати за работа

☐ жалбоподатели

☐ членове и поддръжници на политически партии

пациенти

☐ учащи

☐ нарушители или заподозрени

☐ деца

☐ хора с увреждания

☐ възрастни хора

☐ граждани на други държави от ЕС

☐ граждани на други държави извън ЕС

☐ други .....

9. Превантивни технически и организационни мерки, предприети от АЛД/ОЛД *(Подробно описание на техническите и организационни мерки преди нарушението)*

.....
.....

10. Потенциални последствия за правата и свободите на засегнатите субекти на данни от нарушението.

10.1 Възможно ли е идентифициране на засегнатите лица? Моля, обяснете:

.....

10.2. Налице ли е загуба на способността да се предоставя критична услуга за засегнатите субекти на данни? Моля, опишете:

.....

10.3. Естество на потенциалното въздействие върху субекта на данните. Моля, опишете:

.....

(Примери: Загуба на контрол над лични данни, ограничаване на права, дискриминация, кражба на самоличност, финансови загуби, засягане на репутацията, загуба на поверителност на личните данни, защитени от професионална тайна, неоторизирано превръщане на псевдонимизирани данни в обикновени данни или други (моля, уточнете)

10.4. Тежест на потенциалното въздействие .....

(незначително - ограничено - значително – максимално. Тук посочете резултата от извършената оценка на въздействието на нарушението по отношение на правата на субектите на данни)

11. Възможно ли е нарушението на личните данни да доведе до висок риск за субектите на данни? *Моля, дайте подробности*.....

12. Опишете действията, които сте предприели или предлагате да предприемете в отговор на нарушението.

.....
.....

13. Предприели ли сте действия за ограничаване на нарушението? *Моля, опишете тези коригиращи действия*

.....

(Описание на мерките, предприети от администратора, за отстраняване на нарушението в рамките на 72 часа и в последствие)

14. Моля, очертайте всички стъпки, които предприемате, за да предотвратите повторение на нарушението и в какъв срок очаквате те да бъдат изпълнени.

.....
.....

15. Уведомили сте субектите на данни за нарушението?

.....
.....

16. Моля, посочете средства за комуникация, които сте използвали за информиране на субектите на данни.

.....
.....

17. Уведомяване на други органи/организации за нарушението:

17.1. За които имате задължение за уведомяване по закон/нормативен акт.

.....

17.2. Други администратори на лични данни, на които сте предавали/изпращали личните данни, засегнати от нарушението.

.....

17.3. Други надзорни органи

.....

18. Данни за администратора на лични данни, засегнат от нарушението

• Име на организацията .....

• ЕИК/БУЛСТАТ Регистрационен номер на компанията (ако е наличен)
.....

• Сфера на дейност .....

(За юридическо лице или публичен орган е достатъчно да бъдат попълнени само от част I, т. 1 „Код по БУЛСТАТ/ЕИК", т. 4 и част II, в случай, че другите данни са част от публичен регистър (регистър БУЛСТАТ и Търговски регистър). Необходимите данни ще бъдат събрани служебно от администрацията на КЗЛД в съответствие с чл. 2 от Закона за електронното управление.)

• Данни за контакт .....

• Длъжностно лице за защита на данните или име и позиция на лицето за контакт относно нарушението

• Електронна поща

• Телефонен номер

• Пощенски адрес

19. Други администратори или обработващи лични данни, свързани с нарушението

19.1. Участие на други администратори или обработващи, свързани с нарушението

ДА ☐ НЕ ☐

19.2. Име и качество на другите участващи страни .....

(Тук се въвеждат име и качество на другата (ите) организация (и), участваща (и) в нарушението, и дават подробности за тяхното участие (попълва се само в случай, че отговорът по-горе е ДА)

УКАЗАНИЯ ЗА ПОДАВАНЕ:

1. Начин за подаване на Уведомлението в КЗЛД:

1.1. Лично, на хартиен носител – в деловодството на КЗЛД на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров" № 2;

1.2. С писмо на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров" № 2, Комисия за защита на личните данни;

1.3. На мейла на КЗЛД - kzld@cpdp.bg. В този случай, Уведомлението трябва да бъде подписано с Квалифициран електронен подпис (КЕП).

1.4. Чрез Системата за сигурно електронно връчване, поддържана от Държавна агенция „Електронно управление". В този случай Уведомлението трябва да бъде попълнено и съответният електронен файл да бъде изпратен чрез тази система.

2. Уведомлението се подава от администратора или от изрично упълномощено от него лице с изрично нотариално заверено пълномощно при представителство от лица или организации или с нарочно адвокатско пълномощно (пълномощното се прилага и е неразделна част от Уведомлението).

3. Адресни данни, които са извън територията на Република България се вписват само в частта „Адрес".

ДАТА: ПОДПИС:

ДО:

Надзорен орган:

.....

На вниманието на

.....

Информация за Администратора

Наименование: Прокуратура на Република България, ЕИК по БУЛСТАТ 121817309

Адрес: София 1061, бул. „Витоша" № 2

Данни за контакт с Длъжностно лице по защита на данните:

Три имена .....

Телефон .....

E-mail .....

Адрес .....

Друга информация за контакт: .....

Описание на естеството на нарушението на сигурността на личните данни:

Дата и час на узнаване на нарушението: .....

Причина за забавяне на уведомяването (*ако има такова*)

.....

Описание

.....

Категории засегнати лични данни

.....

Засегнати субекти (*категории и приблизителен брой*)

.....

Засегнати записи на лични данни (*приблизителен брой*)

.....

Последици от нарушение на сигурността на личните данни

.....

Поетапно подаване на информация – ДА / НЕ

.....

Предприети или предложени от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност, мерки за намаляване на евентуалните неблагоприятни последици

.....

Доказателства (описание)

.....

Оценка на риска/ технически организационни мерки

.....

Дата: Подпис

Настоящото уведомление е примерно, доколкото КЗЛД не е утвърдила образец на подобно уведомление. В случай че такава бланка на надзорния орган е налице, настоящата бланка не следва да бъде използвана. Минималните изисквания към съдържанието на уведомлението са описани в чл. 33, пар. 3 от ОРЗД.

Приложение № 23
Политика за защита на лични данни

СЪОБЩЕНИЕ ЗА НАРУШЕНИЕ ОТ АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ ДО СУБЕКТА НА ДАННИ

ДО

……..

СЪОБЩЕНИЕ
за нарушение на сигурността на личните данни на основание чл. 34, пар. 1 от Регламент (ЕС) 2016/679 от Прокуратурата на Република България

УВАЖАЕМИ ГОСПОДИН/ГОСПОЖО …..

На …….. (*посочва се датата/моментът, в който администраторът е узнал, че е настъпило нарушение на сигурността*) Прокуратурата на Република България установи, че е настъпило нарушение на сигурността на личните данни, от което съществува вероятност да бъде породен висок риск за правата и свободите на физическите лица, чиито данни са обект на нарушение. Тъй като Вие сте сред тези лица, на основание чл. 34, пар. 1 от Регламент (ЕС) 2016/679 Ви предоставяме следната информация:

1.Естество на нарушението

Нарушението се изразява в ……

Нарушението засяга следните категории лични данни:

2.Координати за връзка с длъжностното лице по защита на данните

За контакт с администратора и допълнителна информация може да се обърнете към ……

3. Евентуални последици от нарушението

Нарушението на сигурността би могло да доведе до следните последици: ……..

4.Мерки за справянето с нарушението на сигурността на личните данни

За справяне с нарушението на сигурността на личните данни сме предприели технически и организационни мерки, както следва: …….

РЕГИСТЪР (*Дневник*) НА НАРУШЕНИЯТА НА СИГУРНОСТТА НА ДАННИТЕ

Съгласно Правилата администраторът има задължението да води регистър на нарушенията.

Регистърът се поддържа от длъжностното лице по защита на данните и трябва да включва всички подробности, свързани с нарушението: причините за нарушението; какво точно се е случило; личните данни, които са били засегнати; последиците от нарушението, както и предприетите действия за справяне с него.

В структурните звена с право на достъп до лични данни се води дневник на нарушенията на сигурността на данните, информацията в който се предоставя на длъжностното лице по защита на данните след всяко настъпило нарушение.

Примерен регистър/дневник на нарушенията на сигурността на данните:

Описание на нарушението	Отговорни лица	Уведомление на надзорния орган	Уведомяване на субекти на данни	Категории нарушени лични данни	Нарушени чувствителни данни	Свързани дейности по обработването	*Уведомяване на главния прокурор или длъжностното лице по защита на данните*

В графа „**Описание на нарушението**“ се посочва:

Вида на нарушението.

Например:

- Пробив в системата за вътрешна комуникация

- Установена липса на данни на хартиен носител (договори, болнични листове и т.н.).

В графа „**Отговорни лица**“ се посочва:

Посочете информация за едно или повече лица, които отговарят за обработването.

Например:

- Структура с право на достъп при администратора;
- обработващ лични данни (ако има);

В случай, че сметнете за нужно, посочете данни и за други лица, които имат отношение към контрола, сигурността и обработването на засегнатите данни.

В графа „**Уведомление на надзорния орган**“ се посочва:

Надзорния орган при нарушаване на сигурността на данните. Уведомлението трябва да бъде направено в 72-часов срок от узнаване на нарушаването. Посочва се датата на която е направено уведомлението, рег. № на документа.

В графа „**Уведомяване на субекти на данни**“ се посочват:

Имената или, ако това е невъзможно, групата или категорията субекти на данните, които са уведомени за настъпилото нарушение, датата на която са уведомени и в каква форма.

В графа „**Категории на нарушени лични данни**“ се посочват:

Категориите лични данни, засегнати от нарушението.

В графа „**Нарушени чувствителни данни**“ се посочват:

Категориите чувствителни данни, засегнати от нарушението (ако има такива).

В графа „**Свързани дейности по обработването**“ се посочват:

Дейностите по обработване, в които участват личните данни на субекта, подал искането.

Графа „***Уведомяване на главния прокурор или длъжностното лице по защита на данните***“ присъства **единствено** в дневниците, които се водят в структурите с право на достъп при администратора. Въз основа на направе-

но уведомление, длъжностното лице въвежда съответната информация в регистъра.

СЪОБЩЕНИЕ ЗА УСЛОВИЯ ЗА ИЗПОЛЗВАНЕ НА БИСКВИТКИ

Уточнения:

- Необходимо е да се създаде самостоятелна лента, която да се появява при първоначално влизане от конкретен браузър на дадено устройство с информация за това, че на сайта се събират бисквитки и най- общо какви са те и защо.
- Към съобщението трябва да има опция за приемане само на технически необходимите (т.е. всички от домейн prb.bg, които са необходими единствено за сесия и визуализация STDXFWSID е такава PHPSESSION и др.; имайте предвид, че има други, които спадат към аналитичните бисквитки от Google).
- Наред с това трябва да има опция за приемане на всички възможни бисквитки към това съобщение.
- И накрая да има опция за управление и настройка на бисквитките, където да се отваря нов прозорец с информацията за самите бисквитки и управлението им според вида.
- Необходимо е да се уточни дали на сайта на ПРБ се използват заедно с бисквитките и обекти за уеб съхранение (web storage).
- Портала https://opendata.prb.bg/odp-ui/#/public/year-stats е подраздел на ПРБ и за него същото трябва да се направи.
- В секцията „Контакти“ заради интерактивната карта се активират повече бисквитки на Google Maps – ако тя остане в този вид е необходимо посетителя на сайта да е приел и тях изрично.

В самостоятелна лента или прозорец излиза следното съобщение.

Нашият сайт използва бисквитки, които са технически необходими за функционирането му. Пълното или частично деактивиране на тези бисквитки може да компрометира използването на сайта. Ако разрешите, ще използваме и аналитични бисквитки, чрез които събираме статистически данни за посещенията Ви с цел да подобрим работата на сайта.

Освен това използваме YouTube, за да показваме видеоклипове. За използваните от YouTube и от социалните медии бисквитки на нашия сайт също се нуждаем от Ваше разрешение. Изберете бутона „Повече информация и управление“, за да персонализирате съответните настройки.

Към съобщението има три опции директно:

- ✓ Разрешавам всички
- ✓ Само технически необходимите бисквитки
- ✓ Повече информация и управление

При стартиране на опцията за повече информация се отваря следното:

Какво представляват бисквитките и обектите за уеб съхранение и защо ги използваме?

С цел предоставянето на персонализирани настройки и адекватна работа на нашия уебсайт и секциите в него, ПРБ има нужда от технология за запаметяване и съхраняване на информация за използването им от Вас. Това става с помощта на т.нар. бисквитки и обектите за уеб съхранение (web storage).

Бисквитките са малки текстови файлове, съдържащи незначителни количества информация и се съхраняват на Вашия компютър, мобилно или друго устройство или в паметта на Вашия уеб браузър. След това използвания от Вас уеб браузър изпраща тези малки текстови файлове към нашия уебсайт при всяко Ваше посещение, като по този начин ни помага да Ви разпознае и съхранява информация за Вашите потребителски предпочитания (език, приели ли сте политиката ни за бисквитки, респ. какви настройки за бисквитките сте избрали, както и други настройки за показване). Същото предназначение имат и обектите за уеб съхранение.

Използването на събраните бисквитки и обекти за уеб съхранение е много ограничено и е свързано с технически цели - подобряване и персонализиране на функционалността на нашия уебсайт. Те не съдържат информация с личен характер и не идентифицират личността на потребителите, като служат единствено за разпознаване на дадено устройство. Информацията, събрана чрез тях, не може да бъде свързана с конкретно лице и не се използва за установяване на самоличността Ви. Въпреки че се отнасят до анонимни данни, ПРБ третира бисквитките и обектите за уеб съхранение като лични данни, като прилагаме по отношение на тях всички стандарти на Общия регламент относно защитата на данните (GDPR).

Всички данни, събрани чрез бисквитките и обектите за уеб съхранение, са изцяло под наш контрол. Ние не ги използваме за цели, различни от посочените в настоящата Политика.

По-подробна информация относно бисквитките и тяхната функционалност можете да откриете на http://www.aboutcookies.org, а за обектите за уеб съхранение: https://en.wikipedia.org/wiki/Web_storage.

Вие можете да контролирате и управлявате бисквитките и обектите за уеб съхранение по различни начини. Имайте предвид обаче, че премахването или блокирането на бисквитките и обектите за уеб съхранение може да повлияе на използването на опции в сайта, като ограничи достъпа Ви до определени техни функционалности или съдържание, или дори да възпрепятства достъпа Ви до тях.

Описание на използваните от нас бисквитки и обекти за уеб съхранение

Детайлно описание на всички бисквитки и обекти за уеб съхранение, използвани в нашия уебсайт, можете да намерите ТУК.

За уточнение от ПРБ:

Избройте ги всички ако смятате за възможно. Добрата практика до момента е наложила в един файл да бъдат описани всички наименования на бисквитките, за какво са те и колко време се съхраняват.

Видове бисквитки, които се използват на сайта www.prb.bg

Настройка и управление

Технически необходими бисквитки

Опции за потребителя – Включени по подразбиране

Тези бисквитки правят възможна коректната работа на нашия сайт, тъй като Ви дават възможност да разглеждате информацията в тях и да използвате техните функции. Например, благодарение на тях Ви показваме информацията на нашия уебсайт на избрания от Вас език и др.

Аналитични бисквитки

Опции за потребителя – Разреши/Откажи

Ние използваме аналитични инструменти, които ни дават възможност да разберем каква е посещаемостта на нашия уебсайт, лесно ли работят нашите

потребители с тях и какво ги интересува от тяхното съдържание. Събраната чрез тези бисквитки информация се използва изключително и само за статистически цели и няма за цел да бъде използвана за лично идентифициране на потребителите. Ние не получаваме никаква информация за Вашите лични данни. Тези бисквитки ни показват кои страници от нашия уебсайт сте разгледали, дали сте ги посетили през мобилно или десктоп устройство и други анонимни данни. Аналитичните инструменти се предоставят от Google Analytics и събраната информация за Вашия IP адрес не се свързва с каквато и да е друга информация, съхранявана от Google.

Бисквитки за прецизно таргетиране

Опции за потребителя – Разреши/Откажи

Тези бисквитки не съхраняват лична информация, а съдържат само информация за това как сте използвали нашия уебсайт. Те могат да бъдат задействани от наши рекламни партньори, за да Ви показват само информация, която е релевантна за Вас. Например, такива са бисквитките на Google, YouTube и др.

Други средства за управление на бисквитките и обектите за уеб съхранение

Освен чрез опциите в предходната секция, Вие можете да контролирате и управлявате бисквитките по различни начини, използвайки Вашия браузър. Можете да изтриете всички бисквитки на Вашето устройство, като изчистите историята на сърфирането във Вашия браузър. Това ще премахне всички бисквитки от всички уебсайтове, които сте посетили. Имайте предвид, че ако изтриете всички бисквитки, предпочитанията, които сте съхранили също ще бъдат изтрити.

За повече информация как да промените настройките на Вашия браузър, за да изтриете, блокирате или ограничите бисквитките, посетете http://www.aboutcookies.org, http://www.cookiecentral.com

Ние използваме услугата Google Analytics с цел получаване на детайлна статистика за посетителите на нашите сайтове. Можете да научите повече за политиката на Google за защита на личните данни и използването на бисквитките на Google Analytics, като посетите следния уебсайт: https://support.google.com/analytics/answer/6004245. Можете да предотвратите използването на бисквитки от Google Analytics, като свалите и инсталирате на Вашия браузър добавката за блокиране на Google Analytics:

https://tools.google.com/dlpage/gaoptout?hl=en.

Също така, можете да поискате от Вашия браузър да изтрие всички обекти за уеб съхранение, записани във Вашето устройство, като следвате указанията, достъпни чрез посочените препратки:

- Firefox
- Internet Explorer
- Microsoft Edge
- Chrome
- Safari
- Opera

Промени в настоящата политика

ПРБ може по своя преценка да променя и допълва настоящата Политика по всяко време. В случай на изменение на тази Политика, ние ще посочим датата на промяна и това изменение ще влезе в сила по отношение на Вас и Вашите данни след датата на това изменение или от друга, изрично посочена по-късна дата.

ОРГАНИЗАЦИЯ

ЗА ПРОВЕЖДАНЕ НА ТРЕНИРОВКИ ЗА РЕАГИРАНЕ НА ИНЦИДЕНТИ, СВЪРЗАНИ СЪС ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ, В ПРБ

I. Въведение

Правото на защита на личните данни е основно право в Европейския съюз. Гарантирането му налага данните да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание.

С Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните) се определят правилата по отношение на защитата на физическите лица във връзка с обработването на лични данни. Наред с другите изисквания, при обработване на лични данни администраторът прилага подходящи технически и организационни мерки, които да гарантират съответно на рисковете за правата и свободите на физическите лица ниво на сигурност. Мерките трябва да са гаранция срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане на лични данни, т.е. да предотвратяват нарушения на тяхната сигурност.

Наличието на правила, процедури и планове във връзка със защитата на личните данни не е достатъчно, за да се гарантира сигурността на обработването. Необходими са теоретични знания и постоянно практикуване на уменията, тъй като най-базовата и ефективна мярка за защита на личните данни е тренираната човешка бдителност.

Периодичните тренировки на служителите на администратора, ангажирани с обработването на лични данни, са подходяща организационна мярка, която има потенциал да предотвратява рискове за защита на личните данни или да ограничава неблагоприятните им последици върху правата на субектите на данни. Тези периодични тренировки се разглеждат като част от мерките по персонална защита на личните данни, разбирана като комплекс от изисквания, които администраторът прилага спрямо лицата, обработващи лични данни по негово указание.

При отчитане на принципа „необходимост да се знае“, всеки служител, ангажиран с дейности по обработване на лични данни, следва да:

- Познава правната уредба в областта на защитата на личните данни, както и правилата, процедурите и плановете, утвърдени за дейността на администратора;
- Разбира източниците и естеството на заплахите за сигурността на личните данни;
- Разпознава признаци на нарушения на сигурността на личните данни и техники/практики, използвани за заобикаляне на установените мерки за сигурност;
- Съобщава за всеки един инцидент, свързан със защитата на личните данни.

Тренировките имат за цел да гарантират, че служителите на администратора, извършващи дейности по обработване на лични данни, притежават необходимата компетентност, за да спазват всички изисквания, произтичащи от европейското и българското законодателство в областта на защитата на личните данни.

2. Основни насоки при организиране и провеждане на тренировки

Цел на всяка тренировка е тя да поддържа вече придобитите умения и същевременно да се стреми да ги подобри. Тренировките също така могат да бъдат използвани и за проверка на нови процедури.

Целите и използваната методика на тренировките са по-важни от сценария за провеждане. Това означава, че тренировката следва да се анализира в контекста на определените предварително цели, а не само на база на определен сценарий. Целите трябва да бъдат - конкретни, измерими, приемливи, реалистични и обвързани със срокове (от англ. S.M.A.R.T - Specific, Measurable, Acceptable, Realistic and Time-bound):

- **Конкретни: целите трябва да бъдат ясни и недвусмислени;**
- **Измерими: трябва да има ясна дефиниция за това, което трябва да се постигне или направи, а както и дали то е било направено по правилния начин, така че успеха или неуспеха да може да бъде измерен;**
- **Приемливи: целите трябва да са приемливи за всички.**
- **Реалистични: целите трябва да бъдат постижими.**
- **Обвързани със срокове: трябва да бъде възможно целта да се постигне до края на тренировката.**

Представените сценарии за тренировки са примерни и се използват за изграждане/затвърждаване на практическите умения за реагиране при различни проявни форми на нарушения, свързани със сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679. Примерните сценарии не изключват възможността за отклонения от тях, в случай, че това способства ефективното постигане на целите на тренировката.

3. Примерни сценарии

Тренировка № 1. Изпълнение на задълженията за документална защита

СЦЕНАРИЙ: На участниците в тренировката се поставя следния казус:

„Разпределена ви е за работа преписка, съдържаща молба от конкретно лице. След получаване на оригинала на преписката установявате, че не можете да откриете хартиения й носител, защото той не се намира на мястото, на което обичайно съхраняване документите, с които работите.

Според вас нарушена ли е защитата на личните данни?

Какви действия ще предприемете?“

ВРЕМЕ ЗА ВЗЕМАНЕ НА РЕШЕНИЕ И РЕАКЦИЯ: 5 минути

ЦЕЛИ:

Да се провери познаването на Правилата за реагиране на сигнали, свързани с нарушения на защитата на личните данни;

Да се провери времето за реакция и пътя за предаване на информацията, свързана със сигурността на обработването на лични данни;

Затвърждаване на уменията на служителите за създаване на ефикасна организация при прилагането на изискванията за защита на личните данни.

Тренировка № 2. Защита при изпращане на лични данни

СЦЕНАРИЙ: На участниците в тренировката се поставя следния казус:

„Изпращате отговор по заявление за достъп до обществена информация на заявител и впоследствие установявате, че сте изпратили отговора на имейла на друго лице.

Има ли неправомерно обработване на лични данни? Ако да, има ли нарушение на сигурността на личните данни и в какво се изразява то?

Какви действия ще предприемете?

Има ли риск и ако да какъв за правата и законните интереси на засегнатите субекти на данни?"

ВРЕМЕ ЗА РЕШАВАНЕ НА КАЗУСА: 10 минути

ЦЕЛИ:

Да се провери познаването на нормативната уредба, свързана с обработването на лични данни и с достъпа до обществена информация;

Да се провери въз основа на какви критерии ще бъде определено наличието и степента на риск за правата на засегнатите субекти на данни.

Тренировка № 3. Свеждане на данните до минимум

СЦЕНАРИЙ: *Установявате, че не е заличен единен граждански номер и подпис в публикувана на интернет страницата декларация за конфликт на интереси.*

Какви действия ще предприемете?

ВРЕМЕ ЗА РЕАКЦИЯ: 5 минути

ЦЕЛИ:

Да се идентифицират всички възможни действия, които могат да бъдат предприети при необходимост от заличаване на лични данни, публикувани до неограничен кръг адресати;

Да се установи времето за реакция и пълнотата на действия, които ще предприемат служителите.

Тренировка № 4. Права на субектите на данни

СЦЕНАРИЙ: *Получавате на служебния ви имейл възражение от лице, че неправомерно се обработват личните му данни.*

Към кого следва да се насочи за разглеждане възражението?

Какъв е срокът за отговор?

ВРЕМЕ ЗА РЕАКЦИЯ: 5 минути

ЦЕЛИ:

Да се провери познаването на правата на субектите на данни по Регламент (ЕС) 2016/679;

Да се установи времето за реакция и пълнотата на действия, които ще предприемат служителите.

Тренировка № 5. Прилагане на технически и организационни мерки за защита на личните данни

СЦЕНАРИЙ: *Изпращате на личната си поща преписка с необезличени лични данни на физическите лица по нея, за да ви е по-удобно за работа, независимо от мерките, предвидени във Вътрешните правила за защита на личните данни. Няколко дни след това нямате достъп до личната ви поща, тъй като е станала обект на хакерска атака. На следващия ден след атаката в медиите е публикувано факсимиле от преписката, на която са заличени личните данни на физическото лице, но са видни адресатите на документа и резолюциите по него.*

Какви действия ще предприемете?

ВРЕМЕ ЗА РЕАКЦИЯ: 5 минути

ЦЕЛИ:

Да се провери познаването на техническите и организационните мерки, въведени за защита на личните данни в структурата на администратора;

Да се установи времето за реакция и пълнотата на действия, които ще предприемат служителите.

Тренировка № 6. Прилагане на технически и организационни мерки за защита на личните данни (разпознаване на социално инженерство)

СЦЕНАРИЙ: *Получавате обаждане на служебния ви телефон, с което лице, представящ се за служител на банка, иска данни относно месторабoтата, длъжността и размера на доходите на ваш колега, който посочва поименно, като уточнява, че информацията е по повод молбата му за отпускане на кредит.*

Ще предоставите ли исканата информация?

ВРЕМЕ ЗА РЕАКЦИЯ: 5 минути

ЦЕЛИ:

Да се провери познаването на техническите и организационните мерки, въведени за защита на личните данни в структурата на администратора;

Да се установи времето за реакция и пълнотата на действия, които ще предприемат служителите.

4. Документиране и отчетност

С цел отчетност и в изпълнение на задачите си по чл. 39, пар. 1, б. „б“ от Регламент (ЕС) 2016/679 да повишава осведомеността и обучението на персонала, участващ в операциите по обработването, и съответните одити, длъжностното лице по защита на данните:

1) изготвя предложение за провеждане на тренировка за реагиране при инциденти, което съдържа датата на провеждане и кръга на участниците;

2) провежда тренировката, като избира подходящ/и сценарий/и според кръга на участниците и целите на тренировката;

3) обобщава резултатите от тренировките съгласно Приложение № 1 и ги съхранява за целите на отчетността по Регламент (ЕС) 2016/679.

Приложение № 1

ОБОБЩЕН РЕЗУЛТАТ

от проведена тренировка на персонала за реагиране при инциденти, свързани със защитата на личните данни

Дата на провеждане	
Участници	
Сценарий	
Цели	
Оценка за постигане на целите	
Необходимост от промени в правилата и процедурите, или приемане на нови правила и	

процедури	
Необходимост от предприемане на други действия	
Планиране на следваща тренировка	