ВЪТРЕШНИ ПРАВИЛА
за мерките за защита на личните данни съгласно Регламент 2016/679
на Адвокатско дружество „Димитър и Делина Спилкови”, Булстат 176961910**.**

I.Общи положения

Чл. 1. (1) Адвокатско дружество „Димитър и Делина Спилкови”, Булстат 176961910, представлявано от адвокат Димитър Спилков – управител, наричано по-долу само „дружеството“, е юридическо лице, регистрирано по Закона за регистър БУЛСТАТ и Закона за адвокатурата.

(2) Дружеството е с адрес на кантората: гр. Пловдив 4000, ул.“С.Врачански“ № 2А, етаж 3.

(3) Електронен адрес на дружеството: dimitarspilkov@gmail.com.

(4)Телефони за контакт: 0894 624 182; 0894 68 38 48

Чл. 2.(1) Като адвокатско дружество, вписано в Пловдивска адвокатска колегия, дружеството осъществява дейността си, съгласно Закона за адвокатурата, Закона за правната помощ и други нормативни актове, възлагащи права и задължения на адвокатите.

(2) Дружеството обработва лични данни във връзка със своята дейност и определя целите и средствата за обработването им. В този случай, дружеството действа като администратор на лични данни.

Чл. 3. Настоящите Вътрешни правила на дружеството уреждат организацията на обработване и защитата на лични данни на контрагентите и партньорите на дружеството, на неговите клиенти, на адвокатите и на служителите, работещи в дружеството, както и на всички други групи физически лица, с които то влиза в отношения при осъществяването на правомощията и дейността си и при осъществяване на правомощията и дейността на адвокатите в дружеството.

II.Дефиниции

Чл. 4. (1) „Лични данни“ означава всяка информация, свързана с идентифициране на 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.

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

(3) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до който се осъществява съгласно определени критерии.

III.Принципи за защита на личните данни

Чл. 5. (1) Дружеството е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.

(2) Като администратор при обработването на лични данни дружеството спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

Чл. 6. (1) Принципите за защита на личните данни са:

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

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

3. ***Свеждане на данните до минимум*** – данните да са подходящи, свързани с и ограничени до необходимото във връзка с целите на обработването;

4. ***Точност*** – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

5. ***Ограничаване на съхранението*** **–** данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

6. ***Цялостност и поверителност*** **–** обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. ***Отчетност*** **–** администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл. 7. Дружеството организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 8. Дружеството прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;

4. Защита на компютърните информационни системи.

IV. Права на субектите, чиито лични данни се обработват

Чл. 9. Правата на субектите на лични данни, съгласно Регламент 2016/679 са следните:

1.*Право на достъп на субекта до личните му данни;*

2.*Право на коригиране или допълване на неточни данни*;

3. *Право на изтриване /"право да бъдеш забравен"/* на лични данни, които се обработват незаконосъобразно или с отпаднало основание (изтекъл срок на съхранение, оттеглено съгласие, изпълнена първоначална цел, за която са били събрани и др.);

4.*Право на ограничаване на обработването* – при наличие на правен спор между дружеството и физическото лице до неговото решаване и/или за установяването, упражняването или защитата на правни претенции;

5. *Право на преносимост на данните* – ако се обработват по автоматизиран начин на основание договор или съгласие. За целта данните се предават в структуриран вид, широко използван и пригоден за машинно четене формат. Правото на преносимост обхваща само данни, предоставени лично от субекта на данни, както и лични данни, генерирани и събрани от неговата дейност;

6. *Право на възражение* – по всяко време и на основания, свързани с конкретната ситуация на лицето, при условие, че не съществуват законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или съдебен процес;

7. *Право да не бъде обект на изцяло автоматизирано решение*, включващо профилиране, което поражда правни последствия за субекта на данните или го засяга в значителна степен.

V.Срокове за обработване и съхранение на личните данни

Чл. 10. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни, които се събират от адвоката във връзка с конкретно дело, по което е защитник или повереник, се съхраняват на хартиен, технически и/или електронен носител за времето, необходимо за изпълнение на правомощията на адвоката и се пазят в продължение на 5 години от приключване на съответното дело, съгласно чл. 47, ал. 1 от Закона за адвокатурата;

(3) Личните данни, които се събират от адвоката във връзка с изпълнение на правата и задълженията му, във връзка с възложената му от клиент/контрагент работа и пълномощия, извън случаите на ал. 1, се съхраняват за времето, необходимо за изпълнение на задълженията му по възложената работа, което се определя конкретно за

всеки отделен случай, като се взема предвид естеството му, и се съхраняват в продължение на 6 месеца от приключване на конкретния случай, в случай че закон не предвижда друг срок за това.

(4) Личните данни, които се събират от дружеството във връзка с уреждането на трудови правоотношения между дружеството и служителите на дружеството, се обработват и съхраняват съобразно сроковете за това, предвидени в Кодекса на труда, Кодекса за социалното осигуряване и други нормативни и подзаконови нормативни актове, приети за тяхното изпълнение.

(5) Събирането, обработването и съхраняването на лични данни в регистрите на дружеството се извършва на хартиен, технически и/или електронен носител.

VI.Основания за обработване на личните данни

Чл. 11. Когато не е налице никоя от хипотезите на чл. 6, пар. 1, т. б-е от Регламент 2016/679, физическите лица, чиито лични данни се обработват от дружеството, в частност от адвоката и/или конкретен служител, подписват формуляр за изрично съгласие за обработка на личните им данни. (Приложение № 1).

VII.Съхранение на личните данни

Чл. 12. (1) Документите и преписките, по които работата е приключила, се архивират и съхраняват, съгласно сроковете, посочени в чл. 10, ал. 2-4 от настоящите правила.

(2) Трайното съхраняване за нуждите на архивирането документи, съдържащи лични данни, се извършва на хартиен и електронен носител, за срокове, съобразени с действащото законодателство.

(3) Документите на хартиен носител се съхраняват в специални шкафове, в заключващи се помещения.

(4) Документите на електронен носител се съхраняват на компютърни системи и/или външни носители на информация. Достъп до архивите имат само адвокатите в дружеството и съответните негови служители, чиито служебни задължения включват операции по обработването на лични данни.

(5)Архивиране на личните данни на технически носител се извършва периодично от адвоката или съответния оторизиран служител с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само адвоката или съответния оторизиран служител, съобразно възложените от закона правомощия.

Чл. 13. (1) Веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от дружеството регистри. Проверките се извършват от комисия, включваща служител на дружеството и един от адвокатите в него. Доклад за резултата от проверката се представя на управителя.
(2) Докладът по ал. 1 трябва да включват преценка на необходимостта за обработка на личните данни или унищожаване.

Чл. 14. С оглед защита на хартиените, техническите и информационните ресурси дружеството, адвокатите и служителите му, са длъжни да спазват правилата за противопожарна безопасност.

VIII.Мерки при установяване на нарушение

Чл. 15. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, адвокатът и/или служителят констатирал това нарушение/инцидент, незабавно и писмено уведомява управителя на дружеството за нарушението/инцидента. Той от своя страна без ненужно забавяне, не по-късно от 72 часа след узнаването и при спазване на изискванията на чл. 33 от Общия регламент относно защитата на данните и Закона за защита на личните данни уведомява Комисията за защита на личните данни.

(2) Управителят на дружеството незабавно съобщава на субекта на данните за нарушението на сигурността на личните му данни, когато има вероятност то да породи висок риск за правата и свободите му.

(3) Управителят или писмено и изрично оправомощен от него служител, или адвокат в дружеството, писмено документира в протокол всяко нарушение на сигурността на личните данни, като включва времето, фактите и данните, свързани с нарушението, последиците от него и предприетите действия за справяне.

IX.Унищожаване на данните

Чл. 16. (1) След постигане целта на обработване на личните данни и изтичане на съответните срокове за съхранение, предвидени в българското законодателство и настоящите правила, или след подаване на обосновано писмено искане в свободен текст за заличаване/коригиране данните на субекта, съдържащи се в поддържаните от дружеството регистри, следва те да бъдат унищожени/коригирани при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, адвокатът или оправомощеният служител прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(3)Унищожаването се осъществява от служител, упълномощен с изричен писмен акт – решение, на управителя на дружеството.
(4) За всяко унищожаване на лични данни се съставя протокол (Приложение 2).

X.Достъп до личните данни

Чл. 17. (1)Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, управителят на дружеството съобщава в 1-месечен срок от подаване на заявлението, респ. искането.
(3) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(4) Трети страни получават достъп до лични данни, обработвани в дружеството, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ, Висш адвокатски съвет, Национално бюро за правна помощ и др.п.).

XI.Достъп до регистрите с лични данни

Чл. 18. (1) Право на достъп до регистрите с лични данни имат само управителят на дружеството, адвокатите в дружеството, съобразно възложените им от закона правомощия, както и служителите на дружеството, чиито служебни задължения, посочени в длъжностните им характеристики, включват операции по обработването на лични данни.

(2) Служители носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от служители може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните служители.

(3) Служителите нямат право да разпространяват информация за личните данни, станала им известна при и/или по повод изпълнение на служебните им задължения.

XII.ТРАНСФЕР НА ДАННИ

Чл. 19. (1) При липса на гаранциите, посочени в чл .44-48 от Общия регламент, прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:

1. Субектът на данните изрично и писмено се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;

2. 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;

3. Предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;

4. Предаването е необходимо поради важни причини от обществен интерес;

5. Предаването е необходимо за установяването, упражняването или защитата на правни претенции;

6. 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;

7. 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.*

XIII.Мерки по осигуряване на защита на личните данни

Чл. 20. ***Физическата защита*** се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 21. (1). Основните ***организационни мерки за физическа защита*** включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни:
3. определяне на организацията на физическия достъп;

(2) Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения и/или защитени шкафове.

(3) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители и адвокати, с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни.

(4) *Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове*, достъпът до които е ограничен само до съответния адвокат и тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(5) *Организацията на физическия достъп до помещения*, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми, контролно-пропускателна система за достъп) до зоните в обекта с ограничен достъп, включително и тези, в които се намират информационните системи. Достъп се предоставя само на адвокатите и служителите, на които той е необходим, за изпълнение на служебните им задължения.

(6) Зони с контролиран достъп са всички помещения на територията на дружеството, в които се събират, обработват и съхраняват лични данни.

(7) *Използваните технически средства за физическа защита* на личните данни в дружеството са съобразени с действащото законодателство и нивото на въздействие на

тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за адвокати и служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения.

(8) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

Чл. 22. (1) Основните ***технически мерки за физическа защита*** включват:

1. Контролно – пропускателна система за достъп до сградата;
2. Използване на ключалки и заключващи механизми в помещенията, в които се съхраняват личните данни;
3. Шкафове.
4. Оборудване на помещенията с пожарогасителни средства.

(2) Документите, съдържащи лични данни, се съхраняват в *шкафове или картотеки, които могат да се заключват*, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).
(3) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва: *ключалки* (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица; заключваеми шкафове и пожарогасителни средства.

Чл. 23. (1). Основните ***мерки за персонална защита*** на личните данни са:

1. Задължение на служителите и адвокатите да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, чрез инструктаж, проведен от дружеството и удостоверен с подписването на протокол за извършен инструктаж за защита на личните данни по образец от всеки служител (Приложение № 3);
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от дружеството;
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..) между служителите, адвокатите и всякакви други лица, които са неоторизирани;
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни (Приложение 3).

Чл. 24. Основните ***мерки за документална защита*** на личните данни, са:

1.Определяне на регистрите, които ще се поддържат на хартиен носител - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на адвокатите в дружеството, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения, процесуално представителство и др..

1.1 На хартиен носител, в съответния законов срок, се съхраняват и всички лични данни на служителите във връзка с изпълнение на законовите норми на трудовото, осигурителното и данъчното законодателство.

2. *Определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите и договорни задължения на адвокатите и съответните служители на дружеството, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка на физическия носител на данните.

3. *Регламентиране на достъпа до регистрите с лични данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на съответния адвокат или оторизиран служител в дружеството, в съответствие с принципа на „Необходимост да знае".

4. *Определяне на срокове за съхранение* - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани и/или до изтичане на определения в действащото законодателство и настоящите правила срок.

5. *Процедури за унищожаване:* Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните) съгласно глава пета „Унищожаване на данните" от настоящите правила.

Чл. 25. (1) ***Защитата на компютърните системи*** в дружеството включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се обработват и съхраняват лични данни.

1. Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено съответният адвокат и конкретният оторизиран служител, като такъв достъп се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае". Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име, парола и настройка на всички работни станции в режим „автоматично заключване на екрана" (при липса на активност повече от 60 секудни), като по този начин гарантира, че само упълномощени служители и адвокати получават достъп до данните за изпълнение на възложените им функции. Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от компютърен специалист, след изрично разрешение от управителя на дружеството. При приключване на работното време адвокатът, съответно служителят, изключва локалния си компютър.

1.1 С цел повишаване сигурността на достъпа до информация служителите и адвокатите задължително променят използваните от тях пароли на всеки 6 /шест/ месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

2. Активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции.

3. Използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният софтуер се контролира, инсталира и поддържа от оторизирани от дружеството лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на компютърен специалист.

4. Забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система, работещият с нея адвокат или оторизиран служител, е задължен да преустанови действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация) до премахване на зловредния софтуер.

5. *Използваният хардуер* за обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на устойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата. При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизна организация се извършва без устройствата, на които се съхраняват лични данни.

6**.** Служителите или адвокатите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

Чл.26. (1) Политика по *създаване и поддържане на резервни копия за възстановяване:*:

1. Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на дейността на адвоката или съответния служител, оправомощен да обработва лични данни.

2. Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

3. Отговорност за архивиране има съответно адвокатът или служителят, който обработва конкретните лични данни.

4. Срокът на архивиране следва да е съобразен с действащото законодателство и настоящите правила.

5.Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

5.1. Основни *електронни носители на информация са*: вътрешни твърди дискове (част от компютърна система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, памет, ленти и други носители на информация, еднократно записваеми носители и др.)

XIV. Права и задължения на обработващия лични данни адвокат или оторизиран служител

Чл. 27. Адвокатът, съответно оторизираният служителят, е длъжен:

1. Да обработва лични данни законосъобразно и добросъвестно;

2. Да използва личните данни, до които има достъп, съобразно целите, за които се събират, и да не ги обработва допълнително по начин, несъвместим с тези цели;

3. Да актуализира при необходимост регистрите на личните данни;

4. Да заличава или коригира личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. Да поддържа личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват и сроковете, предвидени в закона и настоящите вътрешни правила.

Чл.28. (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен адвокат или служител по обработване на лични данни са произтекли вреди за дружеството или за конкретно трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

XV.Оценка на въздействие

Чл. 29. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, дружеството може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

Чл. 30. (1) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването дружеството, в частност управителят, в екип от един адвокат в дружеството, оправомощен от управителя, извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни, по критерии, конкретно предвидени за съответния случай.

(2) Оценката по ал. 1 съдържа най-малко общо описание на предвидените операции по обработване, оценка на рисковете за правата и свободите на субектите на данните, мерките, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни и за доказване на съответствие с правилата на защита на личните данни съгласно РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица (Общ регламент относно защитата на данните), на Закона за защита на личните данни (ЗЗЛД) и подзаконовите нормативни актове, приети за неговото изпълнение, като се вземат предвид правата и легитимните интереси на субектите на данните и другите засегнати лица.

(3) Когато оценката на въздействието покаже, че обработването ще породи висок риск по смисъла на Общия регламент относно защитата на данните, на Закона за защита на личните данни (ЗЗЛД) и подзаконовите нормативни актове, приети за неговото изпълнение, се провежда консултиране с Комисията за защита на личните данни преди извършване на обработването.

XVI. Поддържани регистри с лични данни и тяхното управление

Чл. 31. Поддържаните от дружеството регистри с лични данни са:

1. *Регистър „Служители“*, в който се вписват следните видове лични данни:

- *Физическа идентичност* – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
- *Социална идентичност* – данни относно образование и допълнителна квалификация, трудова дейност и професионална биография;
- *Икономическа идентичност* – информация за номер на банкова сметка, с оглед превеждане на трудово възнаграждение по банков път;
- *Лични данни относно съдебното минало на лицето* (свидетелство за съдимост в зависимост от длъжността);
- *Данни за здравословно състояние* – медицинско свидетелство, данни, съдържащи се в болнични листове, представяни от самите служители като субекти на данните, решения на ТЕЛК/НЕЛК и др.п., с оглед характера на заеманата длъжност.

2. *Регистър “Контрагенти, клиенти и партньори“,* в който се вписват следните видове лични данни:

- *Физическа идентичност* – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
- *Икономическа идентичност* – обща банкова информация, информация за номер на банкова сметка, ако е необходима, с оглед на конкретния контрагент, клиент, партньор.

XVII.Допълнителни разпоредби

Чл. 32. Всички адвокати и служители в дружеството, както и ръководството на дружеството, са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност, възложената им работа и изпълнение на правомощията им.

Чл. 33. Дружеството има правото да промени политиката си за защита на лични данни по всяко време, без предизвестие, при спазване на законовите изисквания, като новите условия ще започват да се прилагат след публикуването им на сайта на дружеството, а именно: www.spilkov.com.

Чл. 34. (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защита на личните данни, (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

§ 1. Специализирани контакти:

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Адрес: София 1592, бул. „Проф. Цветан Лазаров” № 2
Център за информация и контакти - тел. 02/91-53-518
Приемна - работно време 9:00 - 17:30 ч.

Електронна поща: kzld@cpdp.bg
Интернет страница: www.cpdp.bg

ЛИЦЕ, ОТГОВАРЯЩО ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ДРУЖЕСТВОТО

Адвокат Димитър Спилков
Адрес на кантора: гр. Пловдив, ул. С. Врачански №2А, ет 3
e-mail: dimitarspilkov@gmail.com
телефон за контакт: 0894 624 182
website:www.spilkov.com

Настоящите вътрешни правила са приети от дружеството на 23.05.2018 г.

Одобрил: (п)

адвокат Димитър Спилков - управител