Утвърдена със Заповед № А-124/2018г.
Председател:

ПОЛИТИКА ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА

Гр.София, 29.05.2018 г.

Съдържание

1. Определения на използваните понятия

Софийски окръжен съд, като администратор на лични данни/Съда/	**СОФИЙСКИ ОКРЪЖЕН СЪД** , **ЕИК 00776541**, със седалище и адрес : Бул.“Витоша“ №2 - работодател на служителите, наети на Трудов договор.
Пряк ръководител	Председател на Софийски окръжен съд или лице назначено със заповед на председателя за изпълнение на такава функция.
Служител	Физическо лице, нает от Софийски окръжен съд.
Ръководство	Председател, заместник председатели, съдебен администратор и всяко друго лице в съда, на което са предоставени ръководни функции и управленска власт.
Политика	Настоящата Политика за сигурност на информацията.
Трета страна или клиент	Физическо лице, юридическо лице или друг субект, необвързан със Софийски окръжен съд.

2. Цел и обхват

2.1. Софийски окръжен съд обработва лични данни, като задължително изискване за изпълнение на правомощията му и законовите му задължения. Непредоставянето на лични данни в тези случаи препятства възможността за предприемане на действия по искания на клиентите на съда. Обработва личните данни, когато доброволно бъдат предоставени за целта.

2.2. Системата за сигурност на информацията в Софийски окръжен съд има за цел да защитава служителите и клиентите на съда от незаконни или вредни действия на физически лица, пряко или косвено, съзнателно или несъзнателно при обработката на информация и лични данни, които са на тяхно разположение, а също така и при употребата на определено оборудване за изпълнение на служебните им задължения.

2.3. Политиката се прилага при обработка на информация в рамките на всяка система или съхранявана на всякакъв носител, участващ в обработката на лични данни/информация в рамките на съда, независимо от това дали обработката на лични данни/информация е свързана с правомощията му и законовите му задължения, или с външни отношения на Софийски окръжен съд с трети страни.

2.4. Настоящата Политика се прилага и по отношение на начина, по който служителите на Софийски окръжен съд използват оборудването и инструментите, с които разполагат за изпълнение на служебните си задължения.

2.5. Политиката може да се прилага във връзка с други политики, регулации, процедури и/или насоки, които с течение на времето са приети и въведени от съда.

3. Класификация на информацията

3.1. Обща класификация на информацията, приложима в рамките на съда:

Категория	**Описание**	**Примери (включително, но неограничено до)**
Публична информация	Информация, която може да бъде обработвана и разпространявана в рамките на съда или извън него без никакво отрицателно въздействие, върху него, неговите клиенти и/или свързани лица.	(a) Информация, достъпна чрез публични ресурси или публично известна по друг начин, освен ако не е станала обществено достояние вследствие на действия на служители в нарушение на правилата за защита на информация/лични данни.
Вътрешна информация	Информация, която може да навреди на интересите на съда и/или неговите служители и клиенти.	(a) Всякакви вътрешни работни бележки, документи, изявления, становища, разработени за нуждите на съда.
Поверителна информация	Всяка информация от такова значение за съда и който и да е от неговите клиенти и/или свързани лица, неоторизираното разкриване на която би могло да възпрепятства бързото, точно и независимо изпълнение по прилагане на законовите му задължения.	(a) Информация, за която е указано на служителя, че е служебна тайна и всяка информация станала достояние на служителите във връзка с изпълнение на трудовите им задължения (b) Друга информация от финансово, кадрово, правно, естество, планове и операции; (c) Данни за лична идентификация; (d) Информация, която подлежи на защита по силата на споразумение за поверителност. (e) Информация, която подлежи на защита по силата на законови и нормативни актове.

4. Системи, заети с обработка на лични данни/информация

4.1. Всякакви информационни системи, включително, но неограничено до компютърно оборудване, всякакъв тип софтуер, операционни системи, всякакви носители за съхранение, мрежови профили, електронни пощенски акаунти, системи за сърфиране и всяка друга техническа база и инструменти, използвани в дейността на съда, се считат за собственост на съда.

4.2. Всеки служител следва да използва такова техническо оборудване и инструменти с дължимата грижа и внимание и само за целите, свързани с дейността на съда. Единственото изключение е техническо оборудване, което изрично позволява и личното му ползване.

5. Задължения на служителите

5.1. Цялата информация/Всички лични данни, която/които е/са на разположение на служителя при изпълнение на служебните му задължения, се считат и се третират като поверителни и като подлежащи на защита в съответствие с тази Политика и няма да се разкриват пред трети лица освен ако ръководството обяви, че това е необходимо или такава/-ива информация/лични данни е/са станало/-и публично достояние, или която вече не подлежи на защитата, установена с настоящата Политика.

5.2. Всички лични данни и друга информация, чрез която физическото лице може да бъде идентифицирано, се събират и обработват само ако се изисква и до степента, необходима за изпълнение на служебните задължения на служителя, при условие, че тези дейности се извършват в рамките на правомощията, предоставени на служителя и в съответствие със законовите изисквания за защита на личните данни (особено в съответствие с изискванията на Регламент (ЕС) № 2016/679 от 27 април 2016 г. 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)).

5.3. Всеки служител следва да се придържа към настоящата Политика, както и да спазва изискванията на приложимите закони и подзаконови актове, независимо дали са местни, регионални или международни, които установяват изисквания за обработка и защита на информацията/личните данни.

6. Управление на достъпа и защитата

6.1. Всички устройства, предоставени на служителите, са достъпни за тях въз основа на техните служебни задължения, отговорности и принципа „необходимост да се знае". Достъпността до която и да е система не означава, че служителят е оторизиран да преглежда или използва цялата информация в рамките на конкретната система.

6.2. Приложните потребителски идентификатори са уникални и идентифицират конкретен служител. Всеки служител е отговорен за всички действия, свързани с неговия/нейния личен идентификационен профил, поради което основното задължение е да се гарантира, че идентификацията на служителя не е на разположение на трети лица и дори на други служители, освен ако съдът е установил различен от този ред.

6.3. Паролите за сигурност на системата се създават с необходимата дължина, при условие, че не са лесни за отгатване, не включват лични данни, се променят редовно (не по-малко от веднъж на 3 месеца). Всеки служител е лично отговорен/-а за съобразяването на паролата за сигурност с тази Политика и всички други правила на съда.

6.4. Служителят осъществява достъп до поверителна/-и информация/лични данни само, ако такова правомощие му е предоставено с трудов договор, длъжностна характеристика и/или изрично упълномощаване.

7. Мерки за сигурност

7.1. Всички лични данни и информация, събрани и обработвани под каквато и да е форма (на хартия, електронна и др.), се подчиняват на изискванията на настоящата Политика и всяка нормативна уредба по отношение на събирането, обработването, защитата и задържането на информацията/личните данни, а съответните документи се съхраняват на безопасно място, определено от съда за период, предвиден от приложимите закони и/или посочен от съда.

7.2. Достъпът до интернет и операциите, извършвани от служителите съгласно изискванията на приложимите закони и подзаконови актове, могат да бъдат филтрирани и наблюдавани от надлежно упълномощен ИТ специалист на съда.

7.3. Всички преносими компютри, както и всички облачни места за съхранение на информация, следва да бъдат одобрени от ИТ специалист на съда и надлежно обезопасени, за да се предотврати неоторизиран достъп.

7.4. Само системите и програмният софтуер, лицензирани и оторизирани от съда, могат да бъдат инсталирани и използвани на оборудване и инструменти, използвани в съда. Преди изтегляне или инсталиране на софтуер на устройства, в притежание на и използвани от служителите за целите, описани в настоящата Политика, трябва да получат разрешение от ИТ специалист.

7.5. В случаите, когато служителите използват домашни устройства за достъп до корпоративни ресурси на съда (електронна поща, онлайн/облачни бази данни), са длъжни да спазват изискванията на настоящата Политика така, както биха използвали оборудване, предоставено им от съда. Съответно, забранява се съхраняването на лични данни и информация, свързани със съда на съответните устройства; всяка обработка на личните данни се разрешава само чрез облачни и онлайн места за съхранение, използвани от съда.

7.6. Строго се забранява използването на обществени устройства за достъп (напр. в интернет кафенета, библиотеки и т.н.), освен ако не се касае за случай на критична и спешна необходимост, свързана с работата и прекият ръководител на служителя е предоставил изричното си писмено съгласие за това действие.

7.7. В случай, че на служителя бъде предоставен достъп до система за съхранение на файлове на клиент или партньор за сътрудничество на съда, служителят е длъжен да използва предоставените от клиента или партньора инструменти за достъп и да спазва предоставените указания за изискванията

за сигурна обработка на информация/лични данни (включително използване на системи за криптиране, пароли, ограничения при използването на данни, използване на специализирани местоположения и т.н.).

7.8. От момента, в който по преценка на съда информацията/личните данни, подлежаща/и на защита, вече не е/са необходима/и за дейността на съда, тази/тези информация/лични данни се заличава/ат, всички техни копия се унищожават и служителите, участващи в обработката на съответната/-ите информация/лични данни, се уведомяват съответно за задължението си да унищожат и върнат на съда информацията/личните данни, които вече не се необходими за изпълнение на служебните им задължения, и по-специално да върнат обратно на съда, да изтрият и да унищожат копията в случай на прекратяване на трудовото правоотношение на съответния служител.

7.9. Никаква/-ви информация/лични данни, посочени в настоящата Политика, няма да се изпращат, препращат или по друг начин предоставят на трета страна, освен ако това не е необходимо за изпълнение на служебните задължения на служителя и до степента, която е необходима за изпълнението на тези задължения. В случай на предаване на лични данни на трети страни, се гарантира, че личните данни са защитени и са взети съответните мерки за сигурност.

7.10. Съдът одитира системите, използвани при обработката на информация/лични данни, за да контролира непрекъснатото спазване на настоящата Политика и приложимите законови изисквания.

8. Забранени дейности

8.1. С изключение на специфично установените изключения, в никакъв случай и при никакви обстоятелства не трябва да се използва оборудване, системи или инструменти, собственост на съда, и неговите клиенти, за цели, които не са свързани с трудовите задължения на служителя и с дейността на съда.

8.2. Следващите дейности са строго забранени, без изключения:

(a) Нарушаване на правата на което и да е лице или дружество, защитени от права на интелектуалната собственост, включително, но не само, инсталиране, копиране, разпространение или съхранение на системите или оборудването на съда на нелицензирани софтуерни продукти, онлайн платформи и всяко друго електронно съдържание, нелицензирано за използване от съда;

(b) Неразрешено копиране на материали, обект на авторско право;

(c) Достъп до лични данни, сървър или профил с цел, различна от дейността или служебните задължения на конкретния служител;

(d) Изнасяне на софтуер, техническа информация, софтуер или технология за криптиране в нарушение на приложимите международни или национални закони и нормативни актове и/или указания на съда;

(e) Изнасяне на всякакви лични данни или информация, които са собственост на съда или са поверителни за него, ако такова изнасяне не се изисква в хода на дейността на съда или при изпълнение на служебните задължения на служителя и/или е в съответствие с вътрешните правила на съда, приложимите закони или подзаконови актове;

(f) Разкриване на паролата за профила на служителя на други лица и разрешаване на използването на такъв профил от други лица;

8.3. Всички инциденти по сигурността или обработването на информация/лични данни или заплахи от инциденти незабавно се съобщават на системния администратор и ръководството, което съответно предприема всички мерки за предотвратяване на евентуални вреди/щети, отстраняване на причинените вреди/щети и възстановяване на предходния безопасен статус.

8.4. Ако е приложимо, ръководството има задължението да осигури по-нататъшното отчитане на нарушаването на сигурността на информацията/личните данни пред съответните органи и физически лица, както е предвидено в приложимите закони и подзаконови актове и/или законите на Европейския съюз.