**Е В Р О Т Е С Т - К О Н Т Р О Л  Е А Д**

София 1517, ул. „Бесарабия”  № 108, тел. (02)  4470 360; тел./факс (02) 8720 596;
www.eurotest-control.bg, E-mail: office@eurotest-control.bg

Утвърдил:…….

инж. Иван Кожухаров

/Изпълнителен Директор/

# ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА „ЕВРОТЕСТ – КОНТРОЛ“ ЕАД

Версия 2

София, 2019 г.

Съдържание

## I. Въведение

Настоящата политика за защита на личните данни се основата на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лиза във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (**Регламент (ЕС) 2016/679**), с който се променя съществуващия правен режим по защита на данните и свободното движение на същите.

Като дружество, регистрирано на територията на Република България и обработващо лични данни на граждани на ЕС, за „Евротест – Контрол“ ЕАД възникват редица задължения, свързани с обработването на личните данни и тяхното свободно движение в съответствие с Регламент (ЕС) 2016/679, актовете по неговото прилагане и действащото национално законодателство.

Всички изменения и допълнения на Политиката за защита на личните данни ще бъдат прилагани след публикуване на актуалното й съдържание на уебсайтовете на Дружеството (www.eurotest-control.bg, www.hotel-astra.bg). Политиката ще бъде на разположение на всички клиенти на Дружеството на хартиен вариант, на местата където се приемат клиенти, съответно на:

- „Координация“, ет. 1, стая 101 в офис сградата
- Рецепция в хотел „Астра“.

Дружество, което обработва като администратор личните данни на своите клиенти и гости на хотел Астра:

**„Евротест – Контрол“ ЕАД**

**ЕИК: 121128591**

**Седалище и адрес на управление: гр. София 1517, ул. Бесарабия №108**

Длъжностно лице по защита на данните:

инж. Иван Кожухаров – Изпълнителен Директор

Тел. за връзка: 0899 99 27 37

e-mail: i.kozhuharov@eurotest-control.bg

За връзка с компетентният надзорен орган:

Комисия за защита на личните данни (КЗЛД)

Лично: на адрес: гр. София, бул. „Проф. Цветан Лазаров“ №2;

с писмо: гр. София, п.к. 1592, бул. „Проф. Цветан Лазаров“ №2;

по факс: 02/9153525;

на e-mail: kzld@cpdp.bg;

чрез уебсайта на КЗЛД на адрес: https://www.cpdp.bg;

## II. Определения

*1. Лични данни* - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано; физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, ЕГН, постоянен или настоящ адрес, IP адрес или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

2. *Специални категории лични данни* - 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.

3. *Администратор* - организация, която сама или съвместно с други определя целите и средствата за обработването на лични данни.

4. *Субект на данни* - всяко живо същество, което е обект на лични данни, съхранявани от организация. Такива са клиентите на „Евротест – Контрол“ ЕАД, гостите на хотел „Астра“, служителите на Дружеството, както и служителите на контрагентите на организацията, когато същите обработват техни лични данни.

5. *Обработване* - 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.

6. *Профилиране* - всяка форма на автоматизирано обработване на лични данни, предназначена за оценяване на определени лични аспекти, свързани с физическо лице, или за анализиране или прогнозиране на изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, местоположение, здраве, лични предпочитания, надеждност или поведение. Това определение е свързано с правото на субекта на данните да се противопостави на профилирането и правото да бъде информиран за наличието на профилиране, на мерките, основаващи се на профилирането, и на предвидените последици от профилирането върху лицето.

7. *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. Администраторът има задължението да докладва на надзорния орган за нарушения на сигурността на личните данни и тогава, когато има вероятност нарушението да има неблагоприятни последици върху личните данни или неприкосновеността на личния живот на субекта на данните.

8. *Съгласие на субекта на данните* - означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субектите на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му личните му данни да бъдат обработени.

9. *Дете* - всяко лице на възраст под 16 години или по-ниска възраст, в случай, че такава бъде определена в националното законодателство по защита на данните. Обработването на лични данни на дете е законосъобразно само ако е получено родителско съгласие или съгласие на настойник.

10. *Трета страна* - физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните и администратора.

11. *Регистър с лични данни* - всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

## III. Декларации

1. „Евротест – Контрол“ ЕАД се ангажира да спазва всички съответни правни актове на ЕС и на Република България като държава-членка на ЕС относно защитата на лични данни, както и защитата на правата и свободите на субектите на данни, чиито данни организациите събират и обработват в съответствие с Регламент (ЕС) 2016/679.

2. Спазването на Регламент (ЕС) 2016/679 е описано от настоящата Политика за защита на личните данни и приложенията към нея, заедно със свързаните с тях процедури и регистри.

3. Регламент (ЕС) 2016/679 и настоящата политика, заедно с приложенията към нея, се прилагат за всички дейности, свързани с обработване на лични данни, и описани в регистъра на дейностите по обработване, включително по отношение на личните данни на клиентите, гостите на хотела, служителите, доставчиците и контрагентите, както и всякакви други лични данни, които Дружеството обработва.

4. Длъжностното лице по защита на данните отговаря за преглеждане на регистъра на дейностите по обработване поне веднъж на всеки две години с оглед на всякакви промени в извършваните от съответната организация процеси, свързани с обработването на лични данни, и всякакви допълнителни законодателни изисквания. Този регистър трябва да бъде достъпен при поискване от страна на надзорния орган.

5. Контрагентите и всички трети страни, които работят с или за Дружеството и които имат или могат да имат достъп до лични данни, трябва да са прочели, разбрали и да са се задължили да спазват настоящата Групова политика.

6. Никоя трета страна не може да има достъп до лични данни, съхранявани от Дружеството, без предварително да е сключила споразумение за поверителност на данните, което налага на тази трета страна задължения, не по-малко обременяващи, от тези, с които се е ангажирало Дружеството, и което дава на съответната организация правото да проверява спазването на споразумението.

## IV. Принципи за защита на данните

Всяко обработване на лични данни трябва да бъде извършвано в съответствие с принципите за защита на данните съгласно разпоредбите на член 5 от Регламент (ЕС)

2016/679. Политиките, стандартите и процедурите - приложения към настоящата Политика, имат за цел да гарантират спазването на тези принципи.

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

**Законосъобразно** – събирането и обработването на лични данни се осъществява единствено на законно основание, така както е определено в чл. 6 на Регламент (ЕС) 2016/679.

**Добросъвестно** – личните данни могат да бъдат обработвани само за целта, с която същите са събрани.

**Прозрачно** - Регламент (ЕС) 2016/679 има повишени изисквания относно това каква информация трябва да бъде достъпна за субектите на данни, което е в обхвата на изискването за "прозрачност". То включва правила относно предоставяне на субектите на данните на информацията по членове 12-14 от Регламент (ЕС) 2016/679. Те са подробни и конкретни и поставят акцент върху изготвянето на известията за поверителност в разбираема и достъпна форма, която трябва да бъде съобщена на ясен и прост език. Конкретната информация, която трябва да бъде предоставена на субекта на данните, включва най-малко:

• данните, които идентифицират съответната организация, данни за контакт,;

• координатите за връзка с длъжностното лице по защита на данните;

• целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

• срокът, за който се съхраняват личните данни;

• съществуването на правата да се изиска достъп, коригиране, изтриване или възражение срещу обработването, както и условията, свързани с упражняване на тези права;

• съответните категории обработвани лични данни;

• получателите или категориите получатели на личните данни;

• когато е приложимо, намерението на администратора да предаде личните данни на трета държава и нивото на защита, осигурявано за данните;

• всякаква необходима допълнителна информация, за да се гарантира добросъвестно обработване.

**Личните данни могат да бъдат събирани единствено за конкретни, изрично указани**

**и легитимни цели.** Данните, получени за конкретни цели, не трябва да бъдат използвани за цел, която се различава от целите, които се съобщават официално на надзорния орган като част от регистъра на дейностите по обработване.

Личните данни трябва да бъдат подходящи, свързани с и ограничени до необходимото за обработването:

• Длъжностното лице по защита на данните носи отговорност за гарантиране, че в съответната организацията не се събират лични данни, които не са строго необходими за целите, за които са получени.

• Всички формуляри за събиране на данни на електронен или хартиен носител трябва да бъдат одобрени от длъжностното лице по защита на данните.

• Длъжностното лице по защита на данните гарантира, че всички методи за събиране на данни са преглеждат поне веднъж на всеки две години, за да гарантира, че събраните данни все още са подходящи и не са в прекомерен обем.

**Личните данни трябва да бъдат точни и да се поддържат актуални, като се полагат всички усилия за своевременното изтриване или коригиране**:

• Данните, които се съхраняват, трябва да бъдат преглеждани и актуализирани, когато е необходимо. Не се съхраняват данни, ако не може основателно да се приеме, че са точни.

• Всички формуляри, чрез които се събират лични данни, включват декларация на субектите, че предоставените данни са точни и актуални.

• Длъжностното лице по защита на данните носи отговорност за гарантиране, че целият персонал е обучен за значението на събиране на точни данни и поддържането им.

• Длъжностното лице по защита на данните носи отговорност за гарантиране, че се прилагат подходящи процедури и политики за поддържане на точни и актуални лични данни, като вземе под внимание обема на събраните данни, бързината, с която те могат да се променят, и всякакви други приложими фактори.

• Най-малко на годишна база длъжностното лице по защита на данните преглежда датите на запазване на всички лични данни, обработвани от съответната организация чрез инвентаризация на данните. Данните, които вече не се изискват в контекста на регистрираната цел ще бъдат изтрити по сигурен начин в съответствие с Процедурата за съхранение и изтриване на данни.

• Длъжностното лице по защита на данните носи отговорност за предоставяне на отговор на исканията за коригиране в рамките на месец в съответствие с Процедура за разглеждане на заявления за упражняване на права на субектите на данни. Този срок може да бъде удължен с още два месеца за комплексни искания. Ако организацията реши да не удовлетвори искането, длъжностното лице по защита на данните трябва да отговори на искането, като обясни мотивите си и предостави информация за правото на подаване на жалба до надзорния орган и търсене на съдебна защита.

• Длъжностното лице по защита на данните носи отговорност за предприемане на подходящи мерки, съгласно които ако на организациите на трети страни са предадени неточни или неактуални лични данни, то същите ще бъдат уведомени, че данните са неточни/ неактуални и не трябва повече да се използва за съобщаване на решения относно съответните лица, като също така носи отговорност за предаване на корекциите на личните данни на третата страна, когато това се изисква.

**Личните данни трябва да бъдат съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по- дълъг от необходимото за обработването.**

• Когато личните данни са запазени след датата на обработване, те ще бъдат сведени до минимум с цел да се запази самоличността на субекта на данните в случай на нарушение на сигурността на данните.

• Личните данни се съхраняват в съответствие със сроковете за съхранение, посочени в Политиката за съхранение на данните, след изтичането на които данните ще бъдат унищожени по сигурен начин.

• Длъжностното лице по защита на данните трябва конкретно да одобри съхраняването на данни, надхвърлящо посочените в Политиката за съхранение на данните срокове, като гарантира, че обосновката е ясно определена в съответствие с изискванията на законодателството за защита на данните. Това одобрение трябва да бъде в писмена форма.

**Личните данни трябва да бъдат обработвани по начин, който гарантира подходящо ниво на сигурност**.

Длъжностното лице по защита на данните извършва оценка на риска, като взема под

внимание всички обстоятелства, свързани с дейностите по обработване на лични данни, описани в регистъра на дейностите по обработване.

При определяне на подходящото ниво на сигурност длъжностното лице по защита на данните също така взема под внимание степента на евентуалните вреди или загуби, които могат да бъдат причинени на лицата, ако възникне нарушение в сигурността на данните, последиците от нарушението и възможното накърняване на репутацията.

При оценяване на подходящите технически мерки длъжностното лице по защита на данните има предвид следното:

• защитен достъп с пароли;

• премахване на права на достъп за USB и други носители с памет на компютри, които имат достъп до лични данни;

• софтуер за проверка за вируси и защитни стени;

• права за достъп въз основа на роли, включително права за достъп, предоставени на временно нает персонал;

• сигурност на локални и широкообхватни мрежи;

• технологии за повишаване защитата на неприкосновеността на личния живот като псевдонимизация и анонимизация.

При оценяване на подходящите организационни мерки длъжностното лице по защита на данните има предвид следното:

• подходящите нива на обучение в организацията;

• мерки, които отчитат надеждността на служителите;

• включване на разпоредби относно защитата на данните в трудовите и/ или гражданските договори;

• определяне на дисциплинарни мерки при нарушение на правилата по защита на данните;

• наблюдение на персонала за спазване на съответните правила за защита на данните;

• проверки на физическия достъп до лични данни в електронен вид и на хартиен носител;

• съхраняване на данни на хартиен носител в заключващи се огнеупорни шкафове;

• ограничаване използването на преносими електронни устройства извън работното място;

• ограничаване използването на лични устройства на служителите, които се използват на

работното място;

• приемане на ясни правила за паролите;

• редовно създаване на резервни копия на лични данни и съхраняване на носителите извън обекта;

• налагане на договорни задължения върху организациите вносители с цел предприемане на подходящи мерки за сигурност при предаване на данни извън Европейска икономическа зона.

## V. Допустимост на обработването на лични данни

1. Лични данни на физически лица се обработват само в някой от следните случаи:
   - Ако физическото лице – субект на данните е дало изрично съгласие за обработване на личните му данни за една или повече конкретни цели;
   - Ако обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключване на договор;
   - Ако обработването е необходимо за спазването на законово задължение, което се прилага спрямо Администратора;
   - Ако обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;
   - Ако обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на Администратора;
   - Ако обработването е необходимо за целите на легитимните интереси на Администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни.

## VI. Права на субектите на данни

1. Субектите на данни имат следните права относно обработването на данни и данните, които са записани за тях:

1.1. да подават искания за достъп на субекта по отношение на естеството на съхраняваната информация и на кого е била разкрита;

1.2.да предотвратяват обработване, което може да предизвика вреди или страдание;

1.3.да предотвратяват обработване за целите на директния маркетинг;

1.4.да бъдат информирани за механизма на процеса за автоматизирано вземане на решения, който ще има значително влияние върху тях;

1.5.да нямат значителни решения, взети само чрез автоматизиран процес, които да имат влияние върху тях;

1.6.да завеждат дела за компенсация, ако са претърпели вреди поради нарушение на Регламент (ЕС) 2016/679;

1.7.да предприемат действия за коригиране, блокиране, изтриване, включително правото "да бъдат забравени", или за унищожаване на неточни данни;

1.8.да поискат от надзорния орган да оцени дали някоя разпоредба на Регламент (ЕС) 2016/679 е била нарушена;

1.9.личните данни да им бъдат предоставени в структуриран, широко използван и пригоден за машинно четене формат и правото тези данни да бъдат прехвърлени на друг администратор;

1.10. да се противопоставя на всякакво профилиране, което се осъществява без съгласие.

**"Евротест – Контрол" ЕАД гарантира, че субектите на данните могат да упражняват горепосочените права в съответствие с Процедурата за разглеждане на заявления за упражняване на права на субектите на данни.**

## VII. Съгласие

За целите на тази политика и дейностите по защита на личните данни, терминът "съгласие" означава:

1. 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 съгласието си по всяко време.

2. Субектът на данните е напълно информиран за планираното обработване и е изразил съгласието си в здравословно психическо състояние и без да му е упражняван натиск. Съгласие, получено по принуда или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване.

Трябва да има активна комуникация между страните с цел доказване на активно съгласие. Не може да бъде заключено, че има съгласие при липса на отговор на съобщение или противопоставяне на общи условия на дадена организация.

## VIII. Сигурност на данните

1. Всички служители носят отговорност да осигурят необходимите условия личните данни, обработвани в рамките на процесите, осъществявани в Дружеството и, за които те носят отговорност, да се съхраняват по сигурен начин и да не се оповестяват на трета страна при никакви условия, освен ако тази трета страна не е специално упълномощена да получава тази информация и не е сключила споразумение за поверителност.

2. Всички лични данни трябва да бъдат достъпни само за лицата, които се нуждаят от тях на принципа "Необходимост да знае". Всички лични данни трябва да бъдат разглеждани с най-висока степен на сигурност и трябва да бъдат съхранявани:

• в стая с контролиран достъп, която се заключва, и/или

• в заключено чекмедже или шкаф, и/или

• ако са в електронен формат, със защитена парола съгласно фирмените изисквания и/или

• на (преносими) електронни носители, които са криптирани.

3. Трябва да се положат грижи за гарантиране, че екраните на не се виждат от други лица, освен от упълномощените служители.

4. Ръчните записи не могат да бъдат оставени на места, където могат да бъдат достъпни за неоторизирани лица.

5. Личните данни могат да бъдат изтрити или унищожени в съответствие с Процедурата за съхранение на данни. Ръчните записи, които са достигнали до крайния срок на запазване, трябва да бъдат унищожени и изхвърлени като "отпадъци от поверителни данни". Твърдите дискове на излишните персонални компютри трябва да

бъдат премахнати и незабавно унищожени.

6. Обработването на лични данни “извън обекта” представлява потенциално по-висок риск от загуба, кражба или вреда на личните данни. Персоналът трябва да бъде специално упълномощен за обработване на данни извън обекта.

## IX. Разкриване на данни

1. „Евротест – Контрол“ ЕАД гарантира, че личните данни не са разкрити на неупълномощени лица - членове от семейството, приятели, правителствени органи и в определени обстоятелства - полицията. Всички служители трябва да бъдат внимателни, когато бъдат помолени да разкрият на трета страна лични данни, съхранявани за друго лице и ще бъдат длъжни да присъстват на специално обучение, което ще им позволи да се справят ефективно с такъв риск. Важно е да се има предвид дали разкриването на информацията е свързано с и необходимо за извършване на дейността на организацията.

2. Всички искания за предоставяне на данни по една от тези причини трябва да бъдат съпроводени от подходящи документи и за всички оповестявания трябва да има специални разрешения от страна на длъжностното лице по защита на данните.

## X. Запазване и унищожаване на данни

1. “Евротест – Контрол“ ЕАД не съхранява лични данни във форма, която да позволява идентифицирането на субекта на данните за период, по-дълъг от необходимото във връзка с целите, за които данните са първоначално събрани.

2. Дружеството може да съхранява данни за по - дълги срокове, ако личните данни ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки с цел да бъдат гарантирани правата и свободите на субекта на данните.

3. Срокът на запазване за всяка категория лични данни е посочен в Политиката за съхранение на данни.

4. Личните данни трябва да бъдат унищожени по сигурен начин в съответствие с Регламент (ЕС) 2016/679. Всяко унищожаване на данни се извършва в съответствие с

Политиката за съхранение на данните и се удостоверява с изготвянето на Протокол.

## XI. Регистър на дейностите по обработване на данни

1. Дружеството въвежда процес за инвентаризация на данни и поток от данни като част от своя подход за справяне с рисковете и възможностите в рамките на целия проект за спазване на Регламент (ЕС) 2016/679, посредством изготвянето Регистър на дейностите по обработване на данни, включващ:

• бизнес процесите, свързани с обработване на лични данни;

• източниците на лични данни;

• категориите субекти на данни;

• категориите обработвани лични данни;

• целите, за които се използва всяка категория лични данни;

• получатели и потенциални получатели на личните данни;

• ролята на организацията в обработката на данни.

2. „Евротест – Контрол“ ЕАД е наясно с всички рискове, свързани с обработването на лични данни.

2.1. Оценява се нивото на риска, свързано с обработването на личните данни. Оценките се извършват в съответствие със Стандарта за оценка на въздействието върху защитата на данните и във връзка с обработването, предприето от други лица от името на организацията.

2.2.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, след консултация с длъжностното лице по защитата на данните, се извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

2.3. Когато в резултат на оценка на въздействието върху защитата на личните данни стане ясно, че ще бъде започнато обработване на лични данни, които биха могли да причинят вреди и/ или страдание на субектите на данните, решението за това дали може да се продължи, трябва да бъде консултирано с длъжностното лице по защита на данните.

2.4.Ако има сериозни притеснения както относно потенциалните вреди или страдание,

така и относно количеството съответни данни, длъжностното лице по защита на данните отнася въпроса до надзорния орган.

2.5.Подходящи проверки ще бъдат избрани и приложени с цел намаляване на нивото на риска, свързан с обработването на индивидуални данни на приемливо ниво с оглед на документираните критерии за приемане на риска от страна на организацията и изискванията на Регламент (ЕС) 2016/679.

## XII. Видеонаблюдение

Информацията от видеонаблюдението като дейност, свързана с обработването на лични данни, ще се съхранява за минимален срок, определен в Политиката за съхранение на данните. Видеонаблюдението се извършва само на изрично означените със съкратени известия за поверителност места на база легитимния интерес на организацията да осигури сигурността на служителите и имуществото си, без по никакъв начин да засяга правата и достойнството на субектите на данни (така например Дружеството няма да осъществява видеонаблюдение в тоалетни помещения, съблекални, зали за почивка и т.н.).